Global Information Assurance Certification Paper

Oracle Database Server Security Audit

GCUX Practical
Version 1.9
Option 2 – Consultant's Report

Performed by
Kevin Wenchel
Goodfellows Security, Inc.
January 2003

Abstract

This report documents the results of a UNIX security audit performed against GIAC Enterprise's Oracle database server. The server resides on the GIAC Intranet and hosts 6 production Oracle database instances. The scope of the audit was restricted to the system administration practices, the operating system configuration, and relevant third party system software configuration. A detailed security analysis of the six Oracle database instances running on the system was beyond the scope of this audit. To identify operating system and configuration vulnerabilities, the Nessus network vulnerability scanner, the Center for Internet Security's CIS Scan tool, and John The Ripper were all run against the server. Vulnerabilities identified by the audit are described in detail and assigned an impact level of high, medium, or low along with a rationalization for that assignment. The report concludes with a list of recommendations for correcting the identified vulnerabilities. Shell code and configuration file examples are provided where appropriate to simplify implementation of the recommendations.

EXECUTIVE SUMMARY **6**
BACKGROUND 6
CONCLUSIONS 6
1 SYSTEM DESCRIPTION **7**
1.1 HARDWARE 7
1.2 ADDITIONAL SOFTWARE 7
1.3 SYSTEM ROLE IN ORGANIZATION 7
1.4 USAGE CHARACTERISTICS 7
1.5 NETWORK ACCESSIBILITY 8
1.6 RISKS AND CONCERNS 8
2. DESCRIPTION OF AUDIT METHODOLOGY **9**
2.1 GENERAL METHODOLOGY 9
2.2 TOOLS 9
2.2.1 Nessus Vulnerability Scanner *10*
2.2.2 CIS Scan *10*
2.2.3 Patchdiag *10*
2.2.4 John The Ripper *10*
2.2.5 Solaris logins Utility *10*
2.2.6 Solaris showrev Utility *10*
2.3 VULNERABILITY IMPACT 11
3. DETAILED ANALYSIS **11**
3.1 OPERATING SYSTEM VULNERABILITIES 11
3.1.1 X Font Service Vulnerability *11*
3.1.2 Priocntl System Call Vulnerability *12*
3.1.3 ToolTalk RPC Database Server Vulnerability *12*
3.1.4 Kodak Color Management Profile Server Vulnerability *13*
3.1.5 CDE Calendar Manager Service Daemon Vulnerability *13*
3.1.6 NFS lockd Daemon Vulnerability *13*
3.2 SECURITY PATCH INSTALLATION/MANAGEMENT 14
3.3 CONFIGURATION VULNERABILITIES 15
3.3.1 Unneeded Boot Services *15*
3.3.2 Unneeded Network Services Running from Inetd *16*
3.3.3 X Server, XDMCP, and CDE Running *16*
3.3.4 World-Writable Files and Directories *17*
3.3.5 File Systems Mounted without nosuid and read-only Options *17*
3.3.6 Missing Logon Banners *18*
3.3.7 Core Dumps Enabled System-wide *18*
3.3.8 Password Aging *18*
3.3.9 World Readable/Executable Home Directories *19*
3.3.10 Rsh Enabled *19*
3.3.11 Sendmail Running *19*
3.4 RISKS FROM THIRD PARTY SOFTWARE 20

3.4.1 Buffer Overflow in Apache *20*
3.4.2 Apache Server Disclosure of .jsa Files *20*
3.4.3 Anonymous Access to Oracle Application Server Dynamic Monitoring Pages *20*
3.4.4 Directory Browsing Enabled on Apache /docs *21*
3.4.5 Printenv CGI Script Enabled *21*
3.4.6 Buffer Overflow Vulnerability in Sudo *21*
3.4.7 Dangerous Script Execution via Sudo *22*
3.5 ADMINISTRATIVE PRACTICES 22
3.5.1 GIAC Security Plan *22*
3.5.2 Account Revocation *22*
3.5.3 Password/Account Auditing *23*
3.6 IDENTIFICATION AND PROTECTION OF SENSITIVE DATA ON HOST 23
3.7 PROTECTION OF SENSITIVE DATA IN TRANSIT 24
3.7.1 Data Transmitted via Administrator Access *24*
3.7.2 Network Backups *24*
3.8 ACCESS CONTROLS 24
3.8.1 Physical Access *24*
3.8.2 Access to Privileged Accounts *25*
3.8.3 Separation of Duties *25*
3.8.4 Least Privilege *26*
3.9 AUDITING 26
3.9.1 Audit Data Capture *26*
3.9.2 Audit Data Review *27*
3.9.3 Audit Data Archive *28*
3.10 BACKUP POLICIES AND DISASTER PREPAREDNESS 28
3.10.1 Backups *28*
3.10.2 Offsite data Storage *28*
3.10.3 Disaster Recovery Procedures *29*

4. CRITICAL ISSUES AND RECOMMENDATIONS 29

4.1 TOP TEN VULNERABILITIES 29
4.1.1 Missing Solaris Security Patches *29*
4.1.2 Vulnerable and Unneeded Network Services *29*
4.1.3 Weak Passwords *29*
4.1.4 Oracle Apache Server Remote Code Execution Vulnerability *30*
4.1.5 Sendmail Daemon Running *30*
4.1.6 Weak File Permissions *31*
4.1.7 Dangerous Sudo Scripts *31*
4.1.8 Audit Data Stored on System *31*
4.1.9 Direct Login to Oracle Account *31*
4.1.10 No Password Aging *32*
4.2 ADDITIONAL RECOMMENDATIONS 32
4.2.1 Create login Banners for FTPD and X *32*
4.2.2 Disable Unneeded Boot Services *33*
4.2.3 Disable Core Files *33*
4.2.4 Mount Data File Systems nosuid *34*
4.2.5 Use SSH For Remote Access *34*

4.2.6 Read World Read/Execute Access on Home Directories....34
4.2.7 Create /var/adm/loginlog....34
4.2.8 Compliance with GIAC Security Policy....34
4.2.9 Apache Information Leak Vulnerability....35
4.2.10 Audit Reports....36
4.2.11 Disable X, XDMCP, and CDE on Server....36
APPENDIX A - NESSUS VULNERABILTY SCAN RESULTS 37
APPENDIX B - CIS SCAN RESULTS....59
APPENDIX C - PATCHDIAG OUTPUT 82
ENDNOTES....88

Executive Summary

Background

GIAC Enterprises, an online E-business specializing in the sale of Fortune Cookies, retained the services of Goodfellows Security to perform a security audit of their UNIX database server. Kevin Wenchel conducted the audit between the dates of January 25 and January 30, 2003. The scope of the audit was restricted to system administration practices, operating system configuration, and third party system software configuration. The audit did not focus on Oracle database security or on the security of GIAC's in-house database applications. GIAC's in-house auditors will perform a database and application audit at a later date.

GIAC management recognizes the strategic importance of applying due diligence in protecting sensitive information systems. However, GIAC's current information security policies are minimal and not strongly enforced. GIAC management is undertaking an effort to reassess and improve their security posture. This audit was performed in an attempt to improve the security of a critical business server while GIAC re-evaluates its overall security posture.

Conclusions

The audit uncovered a number of vulnerabilities on the database server that directly threaten the integrity and confidentiality of business data. Any individual with access to GIAC's Intranet and with sufficient motivation can exploit these vulnerabilities. The following is a summary of recommendations that address the most critical security vulnerabilities. These recommendations should be acted on immediately.

- Several accounts have weak or missing passwords. These accounts should be locked pending further review of whether the accounts are needed.

- The server is running several vulnerable network services that could allow a remote attacker to gain full control of the server. These services are unneeded and should be disabled immediately.

- The Apache web server contains a vulnerability that allows a remote attacker to take control of a privileged database administration account. The web server should be patched immediately.

- Weak file permissions exist on several critical application code trees, allowing anyone with local access to the system to overwrite the files with Trojans. These file permissions must be corrected.

- The system has not been patched in a month and several critical security patches are missing from the system. The latest SUN recommended patch bundle should be applied to the system.

1 System Description

1.1 Hardware

Machine Name	Roarke
Server Model	SUN E4500
Operating System	Solaris 8
Processors	4 UltraSPARC II 400MHz processors
Memory	4 Gig memory

Table 1 - System Description.

1.2 Additional Software

The following software packages are installed on the server.

- IPFilter 3.4.18
- Sudo 1.6.3p6
- OpenSSL 0.9.6h
- OpenSSH 3.5p1
  - (OpenSSL 0.9.6h)
  - (zlib 1.1.4)
- Oracle RDBMS 9.0.2
- Oracle Application Server (OAS) 9i (1.0.2.2.2)
  - Apache/1.3.19
    - mod_plsql/3.0.9.8.3
    - cmod_fastcgi/2.2.10
    - mod_perl/1.25
    - mod_oprocmgr/1.0
- Legato NetWorker client 6.1.1

1.3 System Role in Organization

This system is responsible for hosting several of GIAC's production business processing applications and databases including contract administration/management, data warehousing, payroll, and procurement. The system hosts 6 Oracle database instances.

1.4 Usage Characteristics

GIAC end users interact with the system though web based applications and client application software. As a result, there are no UNIX accounts on the server for individuals other than the System Administrators, Operators, and Database Administrators. While the availability of the system is important, there is not a strict 24 by 7 uptime requirement. Availability is absolutely required between the business hours of 9AM-5PM.

1.5 Network Accessibility

As depicted in figure 1, the server resides within GIAC's Intranet and is not directly accessible from the Internet.

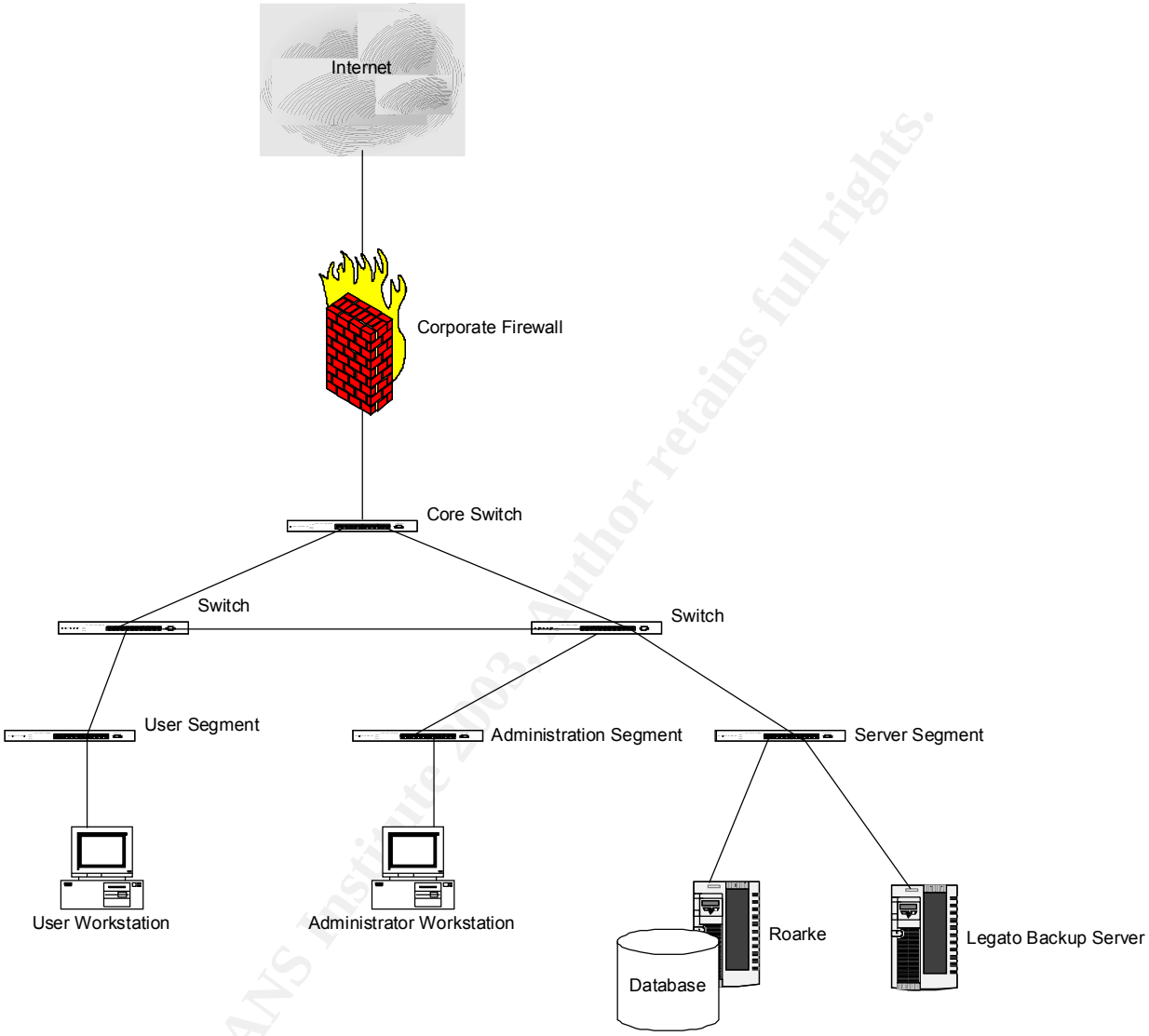

Figure 1 – GIAC Network Architecture.

1.6 Risks and Concerns

The primary concern when auditing the server is to ensure that adequate technical and procedural controls are in place to prevent and detect unauthorized attempts to gain access to the sensitive business data processed on the server. The business data contained on the server is considered "GIAC Sensitive", and access to it is granted on a need to know basis only. Although the server is not directly accessible from the Internet,

a wide variety of individuals from employees, to summer-hires, to visiting consultants and partners have access to the GIAC Intranet and can potentially access the server.

2. Description of Audit Methodology

2.1 General Methodology

The audit was conducted in three phases. The first phase involved a review of the organization's relevant practices, policies, and procedures, where they existed, including:

- Information Security Policy[1].
- System Management Practices and Procedures.
- Disaster Recovery Procedures[2].

In some cases, policies and procedures were informal and did not exist in written form. Staff members were interviewed where necessary to determine current practices and procedures.

The second phase of the audit involved running automated vulnerability scanners against the system to identify obvious vulnerabilities. First, I ran the Nessus network vulnerability scanner against the server to identify the network services running on the machine as well as determine possible remote vulnerabilities. Next, I ran the John the Ripper password-cracking tool against the server to identify accounts with weak passwords. In addition I used the Center for Internet Security's (CIS) Solaris benchmark tool to identify security issues related to the basic system configuration. Finally, I used the SUN Patchdiag tool to identify Sun recommended patches that were absent from the system.

The third phase of the audit involved manually reviewing a number of critical system and application configuration files to identify vulnerabilities that the automated scanning tools may not detect. This included a review of the following files:

- /etc/sudoers
- httpd.conf
- sshd_config
- ssh_config
- crontabs for root and oracle accounts
- IP Filter (/etc/opt/ipf/ipf.conf,/etc/opt/ipf/ipf.nat)

Phases 2 and 3 of the audit also attempted to verify compliance with the policies and procedures disclosed in phase 1.

2.2 Tools

A short description of the tools used in performing the audit follows.

2.2.1 Nessus Vulnerability Scanner

The Nessus vulnerability scanner is an open-source network vulnerability scanner. I ran Nessus version 1.2.7 against Roarke using the default settings and with all plug-ins enabled except dangerous plug-ins. I performed the Nessus scan from a machine located on the administrative network segment. Appendix A lists the report output from the Nessus scan.

2.2.2 CIS Scan

The Center for Internet Security (CIS) developed a benchmark intended to define a best-practice security configuration for the Solaris Operating Environment. In conjunction with the benchmark, CIS released a non-intrusive, host-based vulnerability scanner, CIS Scan, which can assess the compliance of a server to these best practices. I ran CIS Scan version 1.3.0 from the root account on the server. Appendix B lists the report output from CIS Scan.

2.2.3 Patchdiag

Patchdiag is a reporting tool that compares the patches currently installed on the system to a list of Sun recommended patches. Sun Microsystems provides the Patchdiag tool free of charge. I ran Patchdiag version 1.0.4 with the January 30, 2003 version of the Patchdiag cross-reference file. Appendix C lists the report output from Patchdiag.

2.2.4 John The Ripper

John The Ripper (JtR) is an open-source password-cracking tool. I ran JtR using the "-single" parameter. When run in this mode, JtR primarily uses information obtained from a user's password database entry when attempting to guess passwords. Before running JtR, the password database and the shadow database were merged using the unshadow utility provided with JtR. The following commands were run from the root account on the server.

```
unshadow /etc/passwd /etc/shadow > passwd.dat
john –single passwd.dat
```

2.2.5 Solaris logins Utility

The Solaris logins command (/usr/bin/logins) displays user account information. I ran the logins command with the "-p" parameter from the root account to display all accounts that have no password.

2.2.6 Solaris showrev Utility

The Solaris showrev command (/usr/bin/showrev), when run with the "-p' parameter, displays information on the patches that have been applied to the system. I ran the showrev command in several instances to determine whether a particular security patch was present on the system.

2.3 Vulnerability Impact

Vulnerabilities discovered in this audit are assigned an impact level of high, medium, or low. The definitions for each impact level are loosely based on those defined by the National Institute of Standards[3].

Impact Level	Characteristics
High	Exploitation of the vulnerability leads directly to a situation in which an attacker may: • view, modify, or delete private data. • gain full control of the system. • gain local access to the system.
Medium	When used in combination with other vulnerabilities, this vulnerability may allow an attacker to: • view, modify, or delete private data. • gain full control of the system. • gain local access to the system.
Low	Exploitation of the vulnerability: • Has no serious consequential impact. • Provides an attacker with sensitive or excessive information that may aide the attacker in locating and exploiting other vulnerabilities.

Table 2 – Vulnerability Impact Definitions.

3. Detailed Analysis

3.1 Operating System Vulnerabilities

3.1.1 X Font Service Vulnerability

The X Font Service running on this system is vulnerable to a buffer overflow attack. According to Sun Microsystems, a local or remote user can exploit this vulnerability to

cause a denial of service or execute arbitrary code under the security context of the X Font Service daemon[4]. The X Font Service daemon runs under the unprivileged *nobody* account. A remote attacker who gains to this account would have a significant foothold from which to probe the machine for local vulnerabilities in an attempt to elevate his privileges. In addition, this account owns several files on local NFS mounted file systems. An attacker who gains access to the *nobody* account would be able to read and alter these files. Given these considerations, the impact of this vulnerability on the server is high. Sun has released a patch to correct this vulnerability, but it has not been applied to the system.

The Nessus vulnerability scanner discovered that the X Font Server was running, warned that it may contain vulnerabilities, and provided the relevant CERT Advisory information[5]. After retrieving the relevant SUN security alert and patch information from Sunsolve, I ran the command "showrev –p | grep 109862" on the system to verify the absence of the recommended patch.

3.1.2 Priocntl System Call Vulnerability

This system is vulnerable to a local attack involving a bug in the priocntl system call. A local user can exploit this vulnerability in order to load their own kernel modules, thereby allowing them to execute code with root privileges[6]. Sun has released a patch to correct this vulnerability, but it has not been applied to the system.

Because exploitation of this vulnerability requires local access to the machine, and considering that only the Operators, Database Administrators, and System Administrators have local access to the system, the impact of this vulnerability is medium. The vulnerability could be used in conjunction with another remotely exploitable vulnerability, such as the one described in 3.1, to elevate an attacker's privileges once he has already obtained local access.

I discovered this vulnerability by searching for Solaris related vulnerabilities in the ICAT CVE metabase[7]. ICAT provided a URL to the appropriate SUN security alert and patch information. I ran the command "showrev –p | grep 108528-18" on the system to verify the absence of the recommended patch.

3.1.3 ToolTalk RPC Database Server Vulnerability

A buffer overflow condition exists in the ToolTalk RPC database server running on this system. The vulnerability allows local and remote users to delete files, cause a denial of service, or execute commands under the security context of the account running the ToolTalk RPC database server[8]. Since this daemon runs as root, the impact of this vulnerability on the system is high. Sun has released a patch to correct this vulnerability, but it has not been applied to the system.

The Nessus vulnerability scanner detected the presence of the ToolTalk RPC database server and warned of past vulnerabilities associated with this daemon. I performed a

search on the phrase “ToolTalk RPC” on the Sunsolve web site to locate up to date vulnerability information for this daemon. After locating Sun Alert Notification 46022, I ran the command “showrev –p | grep 110286” on the system to verify the absence of the recommended patch.

3.1.4 Kodak Color Management Profile Server Vulnerability

The Kodak Color Management Profile Server daemon (KCMS_server) running on the server contains a vulnerability that allows local and remote users to retrieve the contents of any file on the system[9]. Currently there are no patches available to correct this vulnerability.

The impact of this vulnerability on the system is high. A remote attacker could exploit this vulnerability to download sensitive data and system files, including the /etc/shadow password database.

The Nessus vulnerability scanner identified the presence of the KCMS server daemon and warned of past vulnerabilities associated with this service. I performed a search on the Sunsolve web site for the string “KCMS” to find up to date vulnerability information.

3.1.5 CDE Calendar Manager Service Daemon Vulnerability

The CDE Calendar Manager Service daemon (rpc.cmsd) running on this server is subject to a data type overflow condition which, according to Sun Microsystems, allows local and remote users to gain root privileges on the system[10]. A remote attacker can exploit the integer overflow condition to alter the allocation size of a memory buffer used by the daemon, thereby leading to a buffer overflow condition[11]. The attacker can then exploit the buffer overflow condition to execute arbitrary commands under the security context of the rpc.cmsd daemon. Because the daemon runs under the *root* account, this vulnerability has a high impact on the server. Sun has released a patch to correct this vulnerability, but it has not been applied to the system.

The Nessus vulnerability scanner identified the presence of the rpc.cmsd daemon and warned of past vulnerabilities in this daemon. A search for the string “rpc.cmsd” on the Sunsolve website revealed a recent Sun security alert. I ran the command “showrev -p | egrep '(108827|109091-06)'” on the system to verify the absence of the recommended patch.

3.1.6 NFS lockd Daemon Vulnerability

The NFS lockd daemon running on this system is vulnerable to an attack that allows unauthorized local and remote users to kill the lockd daemon[12]. The lockd daemon is required by NFS to perform record-locking operations on both remotely mounted NFS file systems and locally shared NFS file systems. Killing the lockd daemon results in a denial of service attack against NFS services. Sun has released a patch to correct this vulnerability, but it has not been applied to the system.

Currently, this server uses NFS to mount remote file systems from a legacy server. A temporary denial of service against the NFS services would present a minor inconvenience, but would not seriously impact business processing. The impact of this vulnerability is considered low.

The Nessus vulnerability scanner discovered this vulnerability. Further information on the vulnerability was obtained by searching Sunsolve for the string "lock". After finding the relevant Sun Security alert, I ran the command "showrev –p | egrep '(109783|111321-03)' on the system to verify the absence of the recommended patches.

3.2 Security Patch Installation/Management

GIAC relies on an informal patch management procedure. Several of the system administrators receive Sun Security Bulletins via email. The patches and workarounds provided in these bulletins are implemented as they become available. In addition, roughly once every 6 months, the System Administrators download and install the latest SUN Recommended Patch Cluster.

GIAC applies new patches to a development system and tests them for a period of 2 weeks to 1 month prior to applying them to the production environment. Before installing any patches, the System Administrators consult the Database Administrators and provide them with a list of patch descriptions. Patches that are believed to present a high risk for interfering with system and application stability and whose absence presents low or no security risk are generally not applied.

GIAC takes adequate measures to ensure patches are tested before they are applied to the production environment. However, the absence of numerous critical security patches, as revealed by the results discussed in section 3.1, indicates that the current patch management procedure is ineffective in protecting the server from security vulnerabilities. Ineffective patch management has directly facilitated the presence of high impact vulnerabilities on the system. Table 3 provides a list of critical security patches that are missing from the system.

Vulnerability	Patch ID	Patch Reference
Priocntl system call	108528-18	http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=108528&rev=18
NFS Lockd	109783-02	http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=109783&rev=02
	111321-03	http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=111321&rev=03

Vulnerability	Patch ID	Patch Reference
X Font Service	109862-03	http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=109862&rev=03
ToolTalk RPC Database Server	110286-10	http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=110286&rev=09
CDE Calendar Manager Service Daemon	108827-30 108901-06	http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=108827&rev=30 http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=108901&rev=06

Table 3 - Missing Security Patches.

3.3 Configuration Vulnerabilities

3.3.1 Unneeded Boot Services

CIS Scan detected a plethora of potentially unnecessary boot services enabled on this system. I pruned the results from CIS Scan against the functional requirements of the machine to produce a more accurate listing of which services were truly unneeded. A list of boot services identified as unneeded on this system follows.

```
/etc/rc2.d/S30sysid.net
/etc/rc2.d/S40llc2
/etc/rc2.d/S47asppp
/etc/rc2.d/S70uucp
/etc/rc2.d/S71sysid.sys
/etc/rc2.d/S71ldap.client
/etc/rc2.d/S72autoinstall
/etc/rc2.d/S72slpd
/etc/rc2.d/S73cachefs.daemon
/etc/rc2.d/S74autofs
/etc/rc2.d/S75flashprom
/etc/rc2.d/S80lp
/etc/rc2.d/S80spc
/etc/rc2.d/S80PRESERVE
/etc/rc2.d/S85power
/etc/rc2.d/S89bdconfig
/etc/rc2.d/S90wbem
/etc/rc2.d/S91afbinit
/etc/rc2.d/S91ifbinit
/etc/rc2.d/S92volmgt
/etc/rc2.d/S93cacheos.finish
/etc/rc2.d/S94ncalogd
/etc/rc2.d/S95ncad
```

/etc/rc3.d/S15nfs.server
/etc/rc3.d/S50apache
/etc/rc3.d/S80mipagent

By default, the Solaris Operating Environment starts a number of unnecessary services at boot time and although these services pose no direct security threat at this time, disabling unneeded services is a recommended measure to protect against yet unknown vulnerabilities. The presence of these services on the system has a low impact on the security of the server.

3.3.2 Unneeded Network Services Running from Inetd

In addition to the vulnerable network services identified in section 3.1, the Nessus vulnerability scanner discovered the presence of several dangerous and generally unneeded network services running from Inetd. The only services running from Inetd that are currently required by GIAC are Telnet, FTP, and Rsh. Table 4 provides a listing of the unneeded Inetd services.

Service	Description
dtspcd	CDE Subprocess Control Service
rpc.rstatd	Kernel Statistics Server
rquotad	NFS Remote Quota Server
sadmind	Solstice Admin Daemon
rexec	Remote Execution Server

Table 4 - Unneeded Inetd Services.

Although all relevant security patches have been applied, and these services are not vulnerable to any known attacks, many of these services have exhibited high impact vulnerabilities in the past and likely will again in the future. For this reason, the security impact of running these services is considered high. These services do not provide functionality that is required for the server's business objectives, and allowing them to run exposes the server to unnecessary risk.

3.3.3 X Server, XDMCP, and CDE Running

The Nessus vulnerability scanner detected that the Sun X server, XDMCP server, and the Common Desktop Environment (CDE) windowing system are all running on this server. The X server runs with root privileges, and although no current vulnerabilities exist, the X server remains a viable target for future exploits. XDMCP provides a mechanism for remote users to login to the server and establish a CDE session, presenting one more access point that must be guarded from unauthorized users. Finally, CDE in conjunction with its various supporting daemons is notorious for security vulnerabilities.

Since this machine is a server and not a workstation, and considering that all administration is done remotely using Telnet and SSH sessions, there is no business need for running an X server and a windowing environment. The immediate security

impact as a result of running these services is low, however, sensible precaution suggests that where possible unneeded network services should be disabled.

3.3.4 World-Writable Files and Directories

CIS Scan discovered a large number of world-writable files on the system. In addition, I discovered a large number of world-writable directories on the system by running the following command:

```
find / -perm –0002 –type d
```

A world-writable file is a file that anyone with local access to the system can modify or delete. In almost all cases, the world-writable files on this system are either application binaries or application log files. Accidental or intentional deletion of an application file could create a denial of service against the application. Even more serious, a malicious individual could replace a world-writable application binary with his own Trojan binary.

World-writable directories allow anyone with local access to the system to add and delete files from that directory regardless of the permissions on the files in that directory. A number of the world-writable directories found on the system contained application binaries. Binary files located in world-writable directories can be easily replaced with Trojans by anyone who has gained local access to the server.

The impact of this vulnerability on the system is medium. An attacker who gains local access to the system can use this vulnerability to destroy data and possibly elevate his privileges.

3.3.5 File Systems Mounted without *nosuid* and read-only Options

CIS Scan revealed that several file systems relegated for holding database files or logfiles, including /var and /orafs01 - /orafs20, are not mounted with the *nosuid* option. While this poses no immediate threat to the security of the server, mounting data only file systems with the *nosuid* option is recommended. Mounting a file system *nosuid* in Solaris prevents set-UID executables and device files on that file system from being executed or operated on respectively.

Also, the CDROM file system is not configured to mount with the *nosuid* option. Anyone with the ability to mount CDROMs on the system could mount a CDROM containing set-UID executables of their own making, thereby allowing them to execute their own code with root privileges.

Finally, the /usr file system is not mounted read only. Mounting /usr read-only can make it more difficult for an attacker who has compromised the system to overwrite system binaries with Trojans.

The impact of these vulnerabilities on this system is low. With the exception of the

CDROM file system mounted without the *nosuid* option, these vulnerabilities do not provide an attacker privileged access to the system or access to private data on the system. However, they may aide an attacker who has already gained local access to the system, allowing him to better hide his activities and/or escalate his privileges. The ability to mount CDROMs is controlled via Sudo and granted to the Database Administrators, who essentially already have full control over the sensitive data that is stored on the system.

3.3.6 Missing Logon Banners

I reviewed the files /etc/default/ftpd and /etc/dt/config/Xaccess and found that warning banners are not displayed prior to logging into FTP or X Windows. The GIAC Security Policy mandates that, where possible, network services must display warning banners. The banner message should not only warn unauthorized users that they are unwelcome on the system, but it should warn all users against misuse of the system. GIAC has configured their Telnet and OpenSSH servers to display appropriate warning messages to users.

There immediate security impact on this server due to these missing banner files is low. However, best practice and GIAC policy dictates that FTPD and X should be configured to display appropriate banners.

3.3.7 Core Dumps Enabled System-wide

CIS Scan discovered that core dumps are enabled on the system. Core files are generated by the system when a program encounters an unrecoverable error such as a memory segmentation fault. Core files contain the contents of memory allocated to a program at the time it crashed and can be helpful when debugging development code. The contents of a core file generated from a database application may include business data and possibly other username/password data. The current system configuration allows core dumps for all non-set-UID executables.

The security impact of this configuration vulnerability is low. An attacker who gains local access to the system though other means may be able to use the information contained in a core file to gain further access to private data on the system. As this is a production environment, there is no reason to allow the generation of application core files.

3.3.8 Password Aging

CIS Scan discovered that password aging is not fully implemented on the system. A maximum password lifetime of 30 days is in effect for all users in accordance with the GIAC security policy; however, no minimum password lifetime is set. Setting a minimum password lifetime prevents a user from flip-flopping passwords. For example, without a minimum password lifetime, a user who has changed his password due to password expiration can immediately afterwards change his password back again to the original password. Setting a minimum password lifetime forces a period of cool down in which

the user cannot change his password.

This has a medium impact on the security of the server. It facilitates bad password practices and increases the system's vulnerability to brute force password guessing attacks.

3.3.9 World Readable/Executable Home Directories

CIS Scan discovered that most all of the home directories on the system are world readable and world executable. This means that anyone with local access to the system can change into any other home directory and attempt to read files. If a user has placed files in his home directory that contain sensitive data and if he has set incorrect permissions on these files or is using an unsafe umask value, these files could potentially be read by anyone with local access to the system.

This vulnerability has medium impact on the security of this system. It potentially allows disclosure of sensitive information and may help an attacker with local access on the system to elevate his privileges.

3.3.10 Rsh Enabled

The Nessus vulnerability scanner and CIS Scan detected that the Rsh daemon is running on the system. The Rsh daemon allows remote users to execute commands on the system. Instead of authenticating the remote client with a username/password combination, the Rsh protocol authenticates the client on the basis of the client's IP address. Because IP addresses can be spoofed, there is a risk when allowing Rsh access that an unauthorized remote user may be able to execute commands on the server. In addition, the data passed between the client and server during an Rsh session is un-encrypted and vulnerable to a sniffing attack.

Rsh is used in a very limited fashion to allow a process running from a legacy server to initiate jobs on Roarke. GIAC has implemented IPFilter rules to restrict Rsh access to only the legacy server to prevent general Rsh use on Roarke. In addition, /.rhosts and /etc/hosts.equiv are not used. The UNIX server and the legacy server reside on a switched network and the data passed over the network from the Rsh command is not sensitive. The security impact of running Rsh in this environment is low. Nonetheless, OpenSSH is a better choice for the job given its availability on Roarke.

3.3.11 Sendmail Running

The Nessus vulnerability scanner detected the presence of the Sendmail daemon listening on port 25. The Sendmail daemon runs with root privileges and has a notorious history full of security vulnerabilities. Many of the past vulnerabilities allowed remote attackers to gain root access on the server.

Several applications running on this server require the ability to receive mail from processes running on other GIAC servers. Since this machine truly does have a business need for running Sendmail, GIAC should consider using IP Filter to restrict access to the Sendmail port. Considering that this server is located within the GIAC Intranet and that the version of Sendmail is not known to have any security vulnerabilities, the immediate security impact is medium. Given the history of Sendmail, it is only a matter of time before a new Sendmail vulnerability is discovered.

3.4 Risks from Third Party Software

3.4.1 Buffer Overflow in Apache

The Nessus vulnerability scanner detected that the system is running a version of Apache that is vulnerable to a buffer overflow attack. The system is running Apache 1.3.19, which was installed as part of the Oracle Application Server product install. Versions of Apache prior to 1.3.24 are vulnerable to a buffer overflow attack that allows a remote attacker to execute commands with the privileges of the account running Apache[13]. After manually reviewing the Apache httpd.conf file, I discovered that the Apache server runs under the local UNIX account *ias*, which is a member of the UNIX *dba* group. The UNIX *dba* group is treated as a privileged group by the Oracle database, and members of the UNIX *dba* group are allowed to login to any database on the local system as the Oracle *sys* user, the Oracle equivalent of the UNIX *root* user.

The impact of this vulnerability on the system is high since it provides a remote attacker the opportunity to gain local access to a UNIX account that can administer any database on the system.

3.4.2 Apache Server Disclosure of .jsa Files

The Nessus vulnerability scanner detected that the Apache server allows anonymous web users to view the contents of *globals.jsa* files. These files are used to define application parameters used by Java Server Pages and may contain sensitive configuration information that could aide an attacker[14].

Currently there are no JSP applications in use by GIAC so the immediate impact of this vulnerability on the server is low. As this may change in the future, however, Apache should be configured to prevent the download of global.jsa files.

3.4.3 Anonymous Access to Oracle Application Server Dynamic Monitoring Pages

The Nessus vulnerability scanner detected that the Apache server allows anonymous web users to access the Oracle Application Server Dynamic Monitoring Server Pages. These pages should not be generally accessible to unauthorized individuals as they give out too much information, and they allow an attacker to monitor the operation of the Oracle server[15].

This vulnerability does not lead directly to unauthorized access, but may aide an attacker by providing excessive information. Therefore, the impact of this vulnerability on the server is considered low.

3.4.4 Directory Browsing Enabled on Apache /docs

The Nessus vulnerability scanner detected that directory browsing is enabled on the Apache /docs directory. This allows anonymous web users to obtain a directory listing for the contents of any directory under /docs that does not contain a file named "index.html".

Currently there are no files in the /docs directory so there is no serious exposure. The impact of this vulnerability on the system is considered low since it could potentially provide a remote attacker with useful information regarding the contents and structure of the docs directory.

3.4.5 Printenv CGI Script Enabled

The Nessus vulnerability scanner detected that the *printenv* CGI script is accessible from the Apache web server by anonymous web users. When accessed, the *printenv* script displays a number of environment variables is use by the web server. Many of the variables displayed provide information regarding local file system paths.

The information disclosed is not itself sensitive, but it may give aide to an attacker. The impact of this vulnerability on the system is low. The *printenv* CGI script is not needed in a production environment and should be disabled.

3.4.6 Buffer Overflow Vulnerability in Sudo

The version of Sudo installed on the system is possibly vulnerable to a buffer overflow attack. By using the –p option and specifying a carefully crafted prompt string with the %h and %u expansion characters, it is possible to cause Sudo to allocate less memory than is actually required to store the prompt string, resulting in memory corruption and possibly the execution of arbitrary commands under the *root* account[16].

The impact of this vulnerability on the system is medium. Although it can lead directly to root access, it can only be exploited from a local account that already has permissions to execute commands through Sudo. In addition, to date this vulnerability has only been exploited successfully on Linux/i386. It is not known whether this vulnerability can be exploited in the Solaris/SPARC environment.

This vulnerability was discovered by first running "sudo –V" to obtain the Sudo version information and then visiting the Courtesan website to check for any known security alerts[17].

3.4.7 Dangerous Script Execution via Sudo

A manual review of the commands configured to run through Sudo revealed a vulnerability that allows certain non-root users to execute arbitrary commands with root privileges. By default, when Sudo executes a command on behalf of a user it does not reset the user's PATH environment variable. Several shell scripts that are currently configured to run via Sudo fail to reset the PATH environment variable, but they reference system commands without using a full path name. If a user with permissions to execute these scripts through Sudo sets their PATH variable to

PATH = /tmp:$PATH

and creates an executable file under /tmp with the same name as a command executed in the script, then the Trojan script under /tmp will execute instead of the real command. The scripts affected by this vulnerability include /usr/sbin/ops_shutdown and /usr/sbin/mount_cdrom. These scripts allow Operators to reboot the system and allow Database Administrators to mount CDROMs respectively.

The impact of this vulnerability is medium. Exploiting this vulnerability requires local access to an account that is granted permission through Sudo to execute the vulnerable scripts. The individuals who are granted access to run these commands through Sudo are already highly trusted. However, if an attacker were able to compromise the password for one of these accounts, he would find a simple backdoor for gaining root privileges on the system.

3.5 Administrative Practices

3.5.1 GIAC Security Plan

The GIAC Information Security Policy dictates that each machine containing "GIAC Sensitive" data must have a written security plan and must have an assigned security officer. The security officer is responsible for performing audits to ensure that the server is managed in compliance with the GIAC Security Policy.

Currently there is no security plan in place for this system. In addition, there is no security officer assigned to this server.

The server is not administered in compliance with the GIAC security policies, and the failure to follow these policies has already had a high impact on the security of this server. Many of the vulnerabilities uncovered during this audit could have been detected and corrected long ago had a security officer been assigned audit responsibility for this system.

3.5.2 Account Revocation

Account revocation for individuals who have terminated employment with GIAC is

efficient. GIAC employs an in-house database application designed to map user accounts to the employees to which they were issued. The application is updated daily with data feeds from the HR database and data feeds from the various UNIX systems, making it possible to generate daily listings of individuals who have been terminated along with the system accounts which were assigned to them. Account revocation is performed daily based on the output of this report. Account revocation consists of using the command 'passwd –l' to lock the user account and then running the command 'passmgmt –m –s /dev/null *username*' to set an invalid shell.

3.5.3 Password/Account Auditing

The John the Ripper password cracking tool found 2 user accounts on the server that had a password equal to the username or the word "password". In addition, the Solaris logins utility found 2 user accounts that had no password. Anyone with access to the GIAC Intranet can log into these accounts. In all four cases the accounts lack any special privileges on the server, and running the finger command against these accounts showed that none of these 4 accounts have been logged into in the past 6 months or longer.

After consulting with the System Administrators, it appears that this situation is partially due to weak administrative practices. In two instances, users had requested to have their passwords reset. The administrator reset the passwords to a simple string, set the account to force a password change at next login, and expected the user to immediately login and reset the password. However, the user never logged in again.

The security impact of accounts with weak or missing passwords is very high as these accounts can be used by anyone to gain unauthorized access to the system.

3.6 Identification and Protection of Sensitive Data on Host

In accordance with GIAC Security Policy, the business data stored on this server is classified as "GIAC Sensitive", meaning that Access to the data is granted on a need-to-know basis only. The majority of the sensitive data on the system resides within the Oracle databases; however, there are a number of sensitive output files and feeder files maintained on the server outside of the databases. The GIAC Security Policy mandates that sensitive information stored on a system must be stored in encrypted form or in compliance with an approved security plan for that specific system. As mentioned in section 3.5.1, there is currently no security plan in place for this system.

Despite to the lack of any formal documentation detailing what sensitive information is stored on the system and how it is protected, it was possible with the assistance of the Database Administrators and System Administrators to track down the files and directories on the system believed to contain sensitive data. Access to the directories and the files containing sensitive information was found to be adequately restricted through the use of access control lists. In several instances sensitive HR data files are stored in encrypted form.

The impact of this vulnerability is medium. By failing to properly identify and document the sensitive information stored on the server, GIAC incurs the risk that sensitive data may be overlooked and hence not properly protected. This could provide an attacker who has gained local access to the system with the ability to view, modify and delete sensitive data.

3.7 Protection of Sensitive Data in Transit

3.7.1 Data Transmitted via Administrator Access

From within the GIAC Intranet, System Administrators, Database Administrators and Operators access the server using Telnet, OpenSSH, or X11. All three mechanisms are available on the system and there is currently no policy stipulating the use of one over the other. Access to the server from beyond the GIAC Intranet is only possible by first authenticating to GIAC's VPN gateway.

Protocols such as Telnet are X11 transmit data across the network in clear text form, exposing data, including passwords, to a sniffing attack. In addition, the Telnet protocol is susceptible to session hijacking in which an attacker could inject commands into another user's Telnet session.

Because the server resides on a private, switched network, the security impact due to the use clear-text protocols is considered low.

3.7.2 Network Backups

The Legato NetWorker product is used to backup this system over the network. No encryption is used when performing the backup. During a backup all of the data on the system is passing over the network in clear text form and is potentially exposed to a sniffing attack. Because the Legato backup server and the Roarke server reside on the same segment of a switched network within the GIAC Intranet, the exposure is considered low.

3.8 Access controls

3.8.1 Physical Access

GIAC has taken adequate measures to ensure the physical security of the server. The server is stored in a machine room located within GIAC's data center building. Access to the data center building is restricted during non-business hours though the use of a badge reader and an electronic lock. The data center building is located within a courtyard, and it is only accessible by first entering through one of several other peripheral GIAC buildings. Access to the peripheral buildings is controlled 24 hours a day by a guard force.

Access to the machine room is controlled with an electronic lock and badge reader, as well as a spin-dial lock. During normal business hours authorized individuals swipe their employee badges through the badge reader to gain entrance. Employees must have their badges specifically authorized before they can access the room. An electronic audit log of all access attempts is maintained. During non-business hours the machine room is locked using a spin-dial lock. Only individuals that have knowledge of the combination can enter the room during this time. Unauthorized employees and visitors are permitted access to the machine room only when a business need exists and only when accompanied by an authorized employee. In addition, these individuals are required to sign a paper log.

3.8.2 Access to Privileged Accounts

Both the *root* and *oracle* UNIX accounts are considered privileged. The *root* account can be accessed only from the system console or by using the su command from an existing session. Direct remote login to the *root* account is not possible. GIAC has restricted access to the su command by implementing the concept of the *wheel* group. Permissions on /usr/bin/su restrict execute access to members of the *wheel* group. Only accounts belonging to the System Administrators are members of this group.

The *oracle* account owns all of the database files and runs all of the database processes on the server, and access to this account provides full administrative access to any database on the server. The *oracle* account is a shared account that is used by several Database Administrators. Database Administrators login directly to the *oracle* account via Telnet from their workstations.

Allowing direct login to the *oracle* account constitutes a vulnerability for two reasons. First, it gives remote attackers the ability to perform exhaustive password guessing attacks against the account. Second, it reduces the effectiveness of the audit trail. Only the IP address from whence an *oracle* login is initiated will appear in the audit trail. In cases where a login session is initiated from another multi-user UNIX machine, there is no way to determine who initiated the login session.

Successfully exploiting this vulnerability depends upon first exploiting other weaknesses. For example, the attacker must obtain the *oracle* password by some means such as sniffing the plaintext password from the network, social engineering, or performing an exhaustive password attack (which should be spotted in the audit logs if proper auditing is being performed). The impact of this vulnerability on the system is medium.

3.8.3 Separation of Duties

Table 5 shows the separation of duties among the four classes of individuals who interact with the system.

Class	Function
System Administrators	Install and maintain system software and hardware. Review system audit logs.
Database Administrators	Install and maintain databases, database software, and database application code. Perform migration of applications from development to production.
Operators	Assist in daily backup procedures. Perform server monitoring.
Developers	Develop in-house applications to support GIAC's business needs.
End Users	Access the applications running from the system in order to perform operation business tasks.

Table 5 - Separation of Duties.

3.8.4 Least Privilege

Root access to this server is given only to the System Administrators. This consists of 5 individuals. Database Administrators and Operators do not have root access and are instead provided with Sudo access for limited activities that require root privileges.

Developers and End Users are not provided with local access to this server. End users access the server through web based applications or client application software.

3.9 Auditing

3.9.1 Audit Data Capture

The primary sources of audit data on the system come from Syslog logging, process accounting, and the Solaris Basic Security Module (BSM) auditing facility. In addition to standard system software, the following third party applications send data to syslog: IPFilter, OpenSSH, and Sudo. Table 6 summarizes the Syslog configuration found in /etc/syslog.conf.

Log Data	Location
*.err;kern.notice;auth.notice	/dev/sysmsg
*.info;mail.none;lpr.none	/var/adm/messages
lpr.info	/var/adm/lpr/log
mail.info	/var/log/syslog
*.alert;kern.err;daemon.err	Operator

Log Data	Location
*.alert	Root
*.emerg	*

Table 6 - Syslog Configuration.

The Solaris BSM kernel auditing policies found in /etc/security/audit_control and /etc/security/audit_user are detailed in table 7.

User	Audit Actions
All Users	Successful/Failed Logins
	Successful/Failed Administrative Actions
	Failed File Creations
	Failed File Deletions
	Failed File Writes
	Failed File Attribute Modification
Root	Successful/Failed File Deletions
	Successful/Failed File Attribute Modification
Oracle	Successful/Failed File Deletions
	Successful/Failed File Attribute Modification

Table 7 - BSM Auditing Policy.

Sufficient audit data is collected on this server for identifying suspicious or malicious user activity and for keeping track of activities performed under the *root* and *oracle* accounts. Traditionally UNIX systems also maintain an audit trail of failed login attempts in the file /var/adm/loginlog. However, failed logins are only logged to this file if it already exists on the system. CIS Scan detected that this file was not present on the system. The absence of this file has a low impact on the security of this server, but it should be created for additional audit trail redundancy.

3.9.2 Audit Data Review

A script run from Cron on a daily basis generates an audit report from the Syslog and BSM audit trails. This report is mailed to each of the System Administrators. GIAC procedures dictate that this report must be reviewed on a daily basis. The audit report contains the following headers:

- Failed Network Logins
- Successful SU Attempts
- Failed SU Attempts
- Buffer Overflow Attempts
- IP Filter Dropped Packets
- .rhosts files (listing of all rhosts files on the system)

The report is missing several important items. First, Sudo usage is not included in the report. Sudo logs both successful and unsuccessful use attempts to Syslog. Unsuccessful Sudo use attempts may indicate malicious activity. Second, the audit report script is written such that failed OpenSSH login attempts do not appear in the report.

The lack of these two items in the audit log presents a medium security risk to the system. Both Sudo and OpenSSH serve as possible targets for attackers and usage of these facilities should be monitored regularly.

3.9.3 Audit Data Archive

Audit data is of the utmost importance for maintaining accountability and aiding forensic analysis in the event of a server compromise. The GIAC Security Policy states that audit data must be retained for 1 year. Currently the audit data from this system is maintained for a 3-year period. Table 8 shows the current audit data archive policy implemented on this server.

Facility	Archived?	Location	Data Retention
Syslog	No		
BSM	Yes	To local disk	3 yrs
Process Accounting	Yes	To local disk	3 yrs

Table 8 - Audit Archive Schedule.

GIAC archives audit data to a hard disk that is attached to the local system. Although access to the archived audit data is restricted to the *root* account, a compromise of the *root* account could result in the deletion or modification of the 3-year sum total of GIAC's audit archive. The impact of this vulnerability on the security of the server is medium.

3.10 Backup Policies and Disaster Preparedness

3.10.1 Backups

The system is backed up using the Legato NetWorker product. A full backup is performed once a week and incremental backups are performed nightly. In addition, the system disk is mirrored nightly to a backup disk in the event that the primary system disk should fail. The ability to restore from the backups has been tested on several occasions both in a test lab and in real life recovery operations.

3.10.2 Offsite data Storage

Copies of the system backups are placed in locked containers and sent to a third party, offsite data protection facility on a daily basis. The system backup tapes remain offsite for a period of 30 days after which time they are returned to GIAC and reused. Data older than one month can no longer be retrieved from backup.

3.10.3 Disaster Recovery Procedures

GIAC has a tested disaster recovery procedure in place. The disaster recovery procedure assumes a non-region wide disaster and assumes that the GIAC building facilities are only partially destroyed.

4. Critical Issues and Recommendations

4.1 Top Ten Vulnerabilities

4.1.1 Missing Solaris Security Patches

The installation of patches is critical to maintaining the security of a system. Two critical components that a successful patch management policy must address include timely patch notification and adequate patch testing and review. GIAC has an informal patch management plan in place that addresses both. Nonetheless, the absence of several critical security patches from the system seems to signal shortcomings in the execution of the current patch management strategy. I recommend that GIAC review their existing approach and develop a written patch management plan that formally sets the expectations and priority of patch management tasks. In the meantime, I recommend GIAC apply the latest SUN recommended patch bundle.

4.1.2 Vulnerable and Unneeded Network Services

A number of the network services running on the system contain vulnerabilities that allow a remote attacker to gain unauthorized local access to the system. The majority of the vulnerabilities are present in network services that are not needed. The only Inetd services required by GIAC at this time are Telnet, FTP, and Rsh. All other Inetd services should be disabled. I recommend running the following commands from a root shell on the system to backup the existing inetd.conf file and create a new one that contains entries for only the required services.

```
cp /etc/inetd.conf /etc/inetd.conf.back
egrep '(in.rshd|in.ftpd|in.telnetd|in.rexecd)' /etc/inetd.conf.back > /etc/inetd.conf
chown root:sys /etc/inetd.conf
kill -1 `ps –e –o pid,comm | grep inetd | cut –d' ' –f1
```

4.1.3 Weak Passwords

Several accounts with weak or missing passwords were found on the system. These accounts allow anyone to gain local access to the system. Once local access is achieved, the attacker can elevate their privileges using one of several local vulnerabilities that currently exist on the system. The following accounts should be locked immediately pending review of whether they are still needed:

jstark

mbishop
rmorris
jkirk

To reduce the risks from weak passwords, GIAC system administrators should implement routine password auditing. The auditing should include running John The Ripper against the UNIX account database on possibly a weekly basis, as well as running the Solaris "logins –p" command to identify accounts without passwords. Because several of the weak passwords resulted from poor administrative practices as discussed in 3.5.3, I would recommend that the administrators decide upon a scheme for generating temporary passwords when setting or resetting user passwords. GIAC must immediately discontinue the practice of setting a password "clear until first login" or resetting an account password to the username.

4.1.4 Oracle Apache Server Remote Code Execution Vulnerability

The version of Apache running on this server is susceptible to a buffer overflow attack that allows a remote attacker to execute commands under the account running the Apache server. The Apache server currently runs under the *ias* account, which is a member of the UNIX *dba* group.

Oracle has released a patch to upgrade the Oracle Apache web server to 1.3.27[18]. I recommend that GIAC apply this patch. In addition, the Apache server should be configured to run under a UNIX account which does not own any files on the system and which is not a member of any privileged UNIX groups. This will help minimize the consequences of a successful buffer overflow attack against the Apache server.

4.1.5 Sendmail Daemon Running

Although the version of Sendmail running on this server is not currently vulnerable, Sendmail's rich history of remote root exploits suggests that future vulnerabilities will be discovered. The Sendmail daemon must run on this server to support a number of business applications that receive incoming mail from other systems. To reduce the risk associated with running Sendmail, access to the Sendmail daemon should be restricted only to the machines that actually have a business need to send email to this server. The following IP filters rules should be added to /etc/opt/ipf/ipf.conf[19].

```
block in from any to roarke port = 25
pass in quick from xxx.xxx.xxx.xxx/xx to 192.168.1.5 port = 25 keep state
```

A "pass in" line like the one shown above should be added for each server that needs access, replacing the xxx.xxx.xxx.xxx/xx with the IP address of the remote server. After adding these rules, issue the following commands from the *root* account to put the new rules into effect.

```
ipf –I –f/etc/opt/ipf/ipf.conf
```

ipf -s

4.1.6 Weak File Permissions

A massive number of world-writable files and directories were uncovered on the system. The majority of these files and directories corresponded to application executables and log files. A remote attacker who has gained unprivileged access to the system would have an easy time escalating his privileges. By replacing application binaries with a Trojan program, an attacker could cause their code to be executed under the security context of an application account. An immediate review of the world-writable files and directories on the system should be undertaken by the System Administrators and Database Administrators in order to identify how to correct the permissions. There is rarely if ever an instance in which an application binary, or the directory that contains it, needs to be world-writable. However, it is possible that some of these weak file permissions were established as a quick fix to get an application up and working instead of attempting to understand the exact requirements of the application and then setting the correct file permissions. For this reason any file permissions changes that are decided upon must first be tested in a development environment.

4.1.7 Dangerous Sudo Scripts

Several scripts that are configured to run with root privileges through Sudo fail to use full path names when referencing system commands and can be exploited to execute arbitrary commands with root privileges. I recommend GIAC rewrite the mount_cdrom and ops_shutdown scripts to use full path names when referencing all commands. The PATH variable should also be reset appropriately at the top of the script to include only /usr/bin and /usr/sbin. Also, the file permissions for shell scripts that execute via Sudo should permit read and execute access only for root. Preventing an attacker from reading the contents of the scripts decreases his ability to successfully exploit vulnerabilities in the scripts.

4.1.8 Audit Data Stored on System

Three years worth of audit data is stored on writable media attached directly to the local system. Although access to the audit data is restricted to the *root* account, a compromise of the *root* account could result in modification or destruction of GIAC's archived audit trails. Even though the audit data is backed up on a nightly basis as part of the daily system backup, only 30 days worth of system backups are maintained. It is recommended that GIAC implement a more comprehensive audit archive solution. At a minimum the archived audit data should be regularly copied to read only media.

4.1.9 Direct Login to Oracle Account

The UNIX oracle account is considered privileged by virtue of the fact that it owns all database files and runs the database processes. Direct login to the oracle account must not be allowed as it diminishes the audit trail and makes possible brute force password

guessing attacks against the oracle account.

Several steps need to be taken to prevent direct login to the oracle account. First, the Oracle account needs to be configured as a "set-UID only" account. To do this, add the value "NP" in the password field for the oracle account in /etc/shadow.

```
oracle:NP:::::::
```

The oracle account must also be prohibited from direct logins using OpenSSH. To do this, add the following line to /usr/local/etc/sshd_config:

```
DenyUser oracle
```

As a final step, add the oracle account to the /etc/ftpusers file. This will prevent the oracle account from logging into the system via FTP.

The easiest solution for providing access to the oracle account is to grant the Database Administrators the ability to execute a shell through Sudo with oracle privileges. To do this, add the following lines to the /etc/sudoers file.

```
Host_Alias   PROD=roark
User_Alias   DBAS= fill in authorized DBA account names here
Cmnd_Alias   ORA_SHELL=(oracle) /usr/bin/ksh
DBAS         PROD=ORA_SHELL
```

4.1.10 No Password Aging

No minimum password lifetime is in effect for accounts on this system. This facilitates bad password practices and increases the system's vulnerability to password guessing attacks. A minimum password lifetime should be configured for the system by setting the MINWEEKS parameter in /etc/default/passwd. GIAC policies dictate a maximum password lifetime of 30 days, so I recommend setting MINWEEKS to 2. Setting this parameter will enable a minimum password lifetime for all new accounts that are created. To enable the minimum password lifetime for existing accounts, the following command must be run from the root account against each user account on the system.

```
passwd –n 14 username
```

4.2 Additional Recommendations

4.2.1 Create login Banners for FTPD and X

Where possible, all network services should display a warning banner. To add a login banner for FTP, create a file named /etc/default/ftpd with the contents:

```
BANNER="Authorized uses only"
```

In order to add a login banner for X Windows, first make a copy of the default Xresources file as shown below.

```
cp /usr/dt/config/C/Xresources /etc/dt/config/C
```

Next, edit /etc/dt/config/C/Xresources, setting the greeting strings to an appropriate warning as shown below:

```
Dtlogin*greeting.labelString:      Authorized uses only
Dtlogin*greeting.persLabelString:  Authorized uses only
```

4.2.2 Disable Unneeded Boot Services

A large number of unnecessary services are configured to start at boot time. These services should be removed from the system startup. The following code, which was derived from the CIS Solaris Benchmark[20], should be run on the system to disable the unneeded boot services.

```
cd /etc/rc2.d
for file in S30sysid.net S40llc2 S47asppp S70uucp S71sysid.sys \
        S71ldap.client S72autoinstall S72slpd S73cachefs.daemon \
        S74autofs S75flashprom S80lp S80spc S80PRESERVE \
        S85power S89bdconfig S90wbem S91afbinit S91ifbinit \
        S92volmgt S93cacheos.finish S94ncalogd S95ncad
do
        [ -s $file ] && mv $file .NO$file
done

cd /etc/rc3.d
for file in S15nfs.server S50apache S80mipagent
do
[ -s $file ] && mv $file .NO$file
done
```

This code will rename the unnecessary startup files to ".NO*servicename*". This will prevent the services from starting at boot time as well as preventing the startup files from appearing when an 'ls' command is run against the directory.

4.2.3 Disable Core Files

Core dumps should be disabled on the system. This can be accomplished by issuing the following command from a root shell[21]:

```
coreadm –d global –d process –d global-setid –d proc-setid –e log
```

This will prevent core files from being generated and will log a message to syslog

whenever a process attempts to dump core.

4.2.4 Mount Data File Systems *nosuid*

It is recommended that all data only file systems be configured to mount with the *nosuid* option. This includes the following file systems:

/orafs01 - /orafs20
/var
/home
/cdrom

For each of these file systems, add the *nosuid* option in the /etc/vfstab as shown in the example below:

/dev/dsk/c6t0d6s0 /dev/rdsk/c6t0d6s0 /orafs01 ufs 2 yes logging, nosuid

4.2.5 Use SSH For Remote Access

The Rsh, Telnet, X11 and FTP protocols are all insecure. All of these protocols transmit data across the network in clear text. They are vulnerable to sniffing attacks and session hijacking attacks. OpenSSH is already installed and properly configured on the server and it is recommended that the System Administrators, Database Administrators and Operators migrate to OpenSSH for all remote access and file transfer activities.

4.2.6 Read World Read/Execute Access on Home Directories

The permissions on all user home directories should be reset to disallow world read and world execute access. The command shown below should be run on the system from the *root* account.

```
chmod o-rwx /home/*
```

4.2.7 Create /var/adm/loginlog

To add redundancy to the audit trail for failed login attempts, the /var/adm/loginlog file should be created. Once created, failed Telnet login attempts will be logged to this file. The shell commands listed below should be run from the *root* account.

```
touch /var/adm/loginlog
chown root:root /var/adm/loginlog
chmod 0600 /var/adm/loginlog
```

4.2.8 Compliance with GIAC Security Policy

It is recommended that GIAC review their own Security Policy and take steps to ensure

that they are in compliance. In particular, GIAC needs to develop an official security plan the server and assign audit responsibility of the server to a security officer.

4.2.9 Apache Information Leak Vulnerability

The Apache web server allows anonymous web users access to potentially sensitive configuration files and sensitive administrative web pages. The ability for anonymous users to download .jsa files and access the Oracle server monitor pages should be restricted. As recommended by CERT, the following directive should be added to the Apache server httpd.conf file to prevent downloads of the globals.jsa file[22].

```
<Files ~ "^\globals.jsa">
  Order allow,deny
   Deny from all
</Files>
```

Security researcher David Litchfield has recommended restricting access to the following URLs in order to prevent anonymous users from accessing sensitive Oracle administrative web pages[23].

```
/dms0
/dms/DMSDump
/servlet/DMSDump
/servlet/Spy
/soap/servlet/Spy
/dms/AggreSpy
/oprocmgr-status
/oprocmgr-service
```

In reality these administrative web pages are rarely used in a production environment, so denying all access to them is acceptable. The following directives should be added to the Apache httpd.conf file to achieve this.

```
<location /dms0>
        order allow,deny
        deny from all
</location>
<location /dms/DMSDump>
        order allow,deny
        deny from all
</location>
<location /servlet/DMSDump>
        order allow,deny
        deny from all
</location>
<location /servlet/Spy>
        order allow,deny
```

```
        deny from all
</location>
<location /soap/servlet/Spy>
        order allow,deny
        deny from all
</location>
<location /dms/AggreSpy>
        order allow,deny
        deny from all
</location>
<location /oprocmgr-status>
        order allow,deny
        deny from all
</location>
<location /oprocmgr-service>
        order allow,deny
        deny from all
</location>
```

4.2.10 Audit Reports

The current audit reports should be modified to include information on Sudo usage attempts and OpenSSH login attempts.

4.2.11 Disable X, XDMCP, and CDE on Server

X, XDMCP, and CDE are running on this server but are not needed. These services should be disabled. To accomplish this run the following command from a root shell on the system:

```
mv /etc/rc2.d/S99dtlogin /etc/rc2.d/.NOS99dtlogin
```

Appendix A - Nessus Vulnerabilty Scan Results

```
Nessus Scan Report
------------------



SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 14
 - Number of security warnings found : 22
 - Number of security notes found : 65



TESTED HOSTS

 roarke (Security holes found)



DETAILS

+ roarke :
 . List of open ports :
   o ftp (21/tcp) (Security notes found)
   o ssh (22/tcp) (Security notes found)
   o telnet (23/tcp) (Security warnings found)
   o smtp (25/tcp) (Security hole found)
   o time (37/tcp) (Security notes found)
   o time (37/udp)
   o sunrpc (111/tcp) (Security notes found)
   o sunrpc (111/udp) (Security notes found)
   o xdmcp (177/udp) (Security warnings found)
   o ldap (389/tcp) (Security hole found)
   o https (443/tcp) (Security notes found)
   o exec (512/tcp) (Security warnings found)
   o biff (512/udp)
   o syslog (514/udp)
   o submission (587/tcp) (Security hole found)
   o unknown (665/tcp) (Security notes found)
   o unknown (898/tcp) (Security hole found)
   o unknown (1526/tcp)
   o unknown (1536/tcp)
   o nfs (2049/tcp) (Security warnings found)
   o nfs (2049/udp) (Security warnings found)
   o unknown (4045/tcp) (Security notes found)
   o unknown (4045/udp) (Security warnings found)
   o x11 (6000/tcp)
   o unknown (6112/tcp) (Security hole found)
   o afs3-rmtsys (7009/tcp)
   o xfs (7100/tcp) (Security hole found)
   o unknown (8009/tcp) (Security hole found)
   o webcache (8080/tcp) (Security notes found)
   o jetdirect (9100/tcp)
```

```
  o unknown (32771/tcp) (Security hole found)
  o unknown (32772/tcp) (Security notes found)
  o unknown (32773/tcp) (Security notes found)
  o general/tcp (Security notes found)
  o general/icmp (Security warnings found)
  o unknown (32796/udp) (Security hole found)
  o unknown (32794/udp) (Security warnings found)
  o unknown (32795/udp) (Security warnings found)
  o unknown (32793/udp) (Security hole found)
  o unknown (32799/udp) (Security hole found)
  o unknown (7937/tcp) (Security notes found)
  o unknown (32924/udp) (Security notes found)
  o unknown (32797/tcp) (Security notes found)
  o unknown (8405/tcp) (Security notes found)
  o unknown (8406/tcp) (Security notes found)
  o general/udp (Security notes found)


. Information found on port ftp (21/tcp)


   An FTP server is running on this port.
   Here is its banner :
   220 roarke FTP server (SunOS 5.8)
    ready.

. Information found on port ftp (21/tcp)


   Remote FTP server banner :
   220 roarke FTP server (SunOS 5.8)
    ready.

. Information found on port ssh (22/tcp)


   An ssh server is running on this
    port


. Information found on port ssh (22/tcp)


   Remote SSH version :
    SSH-2.0-OpenSSH_3.5p1

. Information found on port ssh (22/tcp)


   The remote SSH daemon supports the following versions of the
   SSH protocol :

     . 1.99
     . 2.0

. Warning found on port telnet (23/tcp)
```

```
   The Telnet service is running.
   This service is dangerous in the sense that
   it is not ciphered - that is, everyone can sniff
   the data that passes between the telnet client
   and the telnet server. This includes logins
   and passwords.

   You should disable this service and use OpenSSH instead.
   (www.openssh.com)

   Solution : Comment out the 'telnet' line in /etc/inetd.conf.

   Risk factor : Low
   CVE : CAN-1999-0619

. Information found on port telnet (23/tcp)


   A telnet server seems to be running on this
    port


. Information found on port telnet (23/tcp)


   Remote telnet banner :
             SunOS 5.8
. Vulnerability found on port smtp (25/tcp) :



   The remote sendmail server, according to its version number,
   may be vulnerable to the -bt overflow attack which
   allows any local user to execute arbitrary commands as root.

   Solution : upgrade to the latest version of Sendmail
   Risk factor : High
   Note : This vulnerability is _local_
    only


. Warning found on port smtp (25/tcp)


   The remote SMTP server
   answers to the EXPN and/or VRFY commands.

   The EXPN command can be used to find
   the delivery address of mail aliases, or
   even the full name of the recipients, and
   the VRFY command may be used to check the
   validity of an account.


   Your mailer should not allow remote users to
   use any of these commands, because it gives
```

```
   them too much information.


   Solution : if you are using Sendmail, add the
   option
    O PrivacyOptions=goaway
   in /etc/sendmail.cf.

   Risk factor : Low
   CVE : CAN-1999-0531

. Warning found on port smtp (25/tcp)


   The remote SMTP server allows the relaying. This means that
   it allows spammers to use your mail server to send their mails to
   the world, thus wasting your network bandwidth.

   Risk factor : Low/Medium

   Solution : configure your SMTP server so that it can't be used as a relay
              any more.
   CVE : CAN-1999-0512

. Warning found on port smtp (25/tcp)



   The remote SMTP server allows relaying for authenticated users.
   It is however possible to poison the logs
    this means that spammers
   would be able to use your server to send their e-mails to
   the world, thus wasting your network bandwidth and getting you
   blacklisted.

   *** Some SMTP servers such as Postfix will display a false positive
   *** here

   Risk factor : Low

   Solution : Disable
    poprelayd

. Warning found on port smtp (25/tcp)



   According to the version number of the remote mail server,
   a local user may be able to obtain the complete mail configuration
   and other interesting information about the mail queue even if
   he is not allowed to access those information directly, by running
    sendmail -q -d0-nnnn.xxx
   where nnnn & xxx are debugging levels.

   If users are not allowed to process the queue (which is the default)
   then you are not vulnerable.
```

```
   Solution : upgrade to the latest version of Sendmail or
   do not allow users to process the queue (RestrictQRun option)
   Risk factor : Very low / none
   Note : This vulnerability is _local_ only
   CVE : CAN-2001-0715

. Warning found on port smtp (25/tcp)


   The remote SMTP server is vulnerable to a redirection
   attack. That is, if a mail is sent to :

     user@hostname1@victim

   Then the remote SMTP server (victim) will happily send the
   mail to :
     user@hostname1

   Using this flaw, an attacker may route a message
   through your firewall, in order to exploit other
   SMTP servers that can not be reached from the
   outside.

   *** THIS WARNING MAY BE A FALSE POSITIVE, SINCE
       SOME SMTP SERVERS LIKE POSTFIX WILL NOT
       COMPLAIN BUT DROP THIS MESSAGE ***


   Solution : if you are using sendmail, then at the top
   of ruleset 98, in /etc/sendmail.cf, insert :
   R$*@$*@$*       $#error $@ 5.7.1 $: '551 Sorry, no redirections.'

   Risk factor :
    Low


. Information found on port smtp (25/tcp)


   An SMTP server is running on this port
   Here is its banner :
   220 ESMTP Sendmail 8.11.6+Sun/8.10.2; Wed, 29 Jan 2003
    17:41:50 -0500
    (EST)

. Information found on port time (37/tcp)


   A time server seems to be running on this
    port



. Information found on port sunrpc (111/tcp)
```

```
   RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is
    running on this
    port


. Information found on port sunrpc (111/tcp)


   RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is
    running on this
    port


. Information found on port sunrpc (111/tcp)


   RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is
    running on this
    port


. Information found on port sunrpc (111/udp)


   RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is
    running on this
    port


. Information found on port sunrpc (111/udp)


   RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is
    running on this
    port


. Information found on port sunrpc (111/udp)


   RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is
    running on this
    port


. Warning found on port xdmcp (177/udp)



   The remote host is running XDMCP.

   This protocol is used to provide X display connections for
   X terminals. XDMCP is completely insecure, since the traffic and
   passwords are not encrypted.

   An attacker may use this flaw to capture all the keystrokes of
   the users using this host through their X terminal, including
```

```
   passwords.

   Risk factor : Medium
   Solution : Disable XDMCP
   CVE : CVE-1999-0385


. Information found on port https (443/tcp)


   An unknown service is running on this port.
   It is usually reserved for
    HTTPS

. Warning found on port exec (512/tcp)



   The rexecd service is open.
   Because rexecd does not provide any good
   means of authentication, it can be
   used by an attacker to scan a third party
   host, giving you troubles or bypassing
   your firewall.

   Solution : comment out the 'exec' line
   in /etc/inetd.conf.

   Risk factor : Medium
   CVE : CAN-1999-0618

. Vulnerability found on port submission (587/tcp) :



   The remote sendmail server, according to its version number,
   may be vulnerable to the -bt overflow attack which
   allows any local user to execute arbitrary commands as root.

   Solution : upgrade to the latest version of Sendmail
   Risk factor : High
   Note : This vulnerability is _local_
    only


. Warning found on port submission (587/tcp)


   The remote SMTP server allows the relaying. This means that
   it allows spammers to use your mail server to send their mails to
   the world, thus wasting your network bandwidth.

   Risk factor : Low/Medium

   Solution : configure your SMTP server so that it can't be used as a relay
              any more.
   CVE : CAN-1999-0512
```

```
. Warning found on port submission (587/tcp)


   The remote SMTP server allows relaying for authenticated users.
   It is however possible to poison the logs this means that spammers
   would be able to use your server to send their e-mails to
   the world, thus wasting your network bandwidth and getting you
   blacklisted.

   *** Some SMTP servers such as Postfix will display a false positive
   *** here

   Risk factor : Low

   Solution : Disable poprelayd

. Warning found on port submission (587/tcp)


   According to the version number of the remote mail server,
   a local user may be able to obtain the complete mail configuration
   and other interesting information about the mail queue even if
   he is not allowed to access those information directly, by running

    sendmail -q -d0-nnnn.xxx

   where nnnn & xxx are debugging levels.

   If users are not allowed to process the queue (which is the default)
   then you are not vulnerable.

   Solution : upgrade to the latest version of Sendmail or
   do not allow users to process the queue (RestrictQRun option)
   Risk factor : Very low / none
   Note : This vulnerability is _local_ only
   CVE : CAN-2001-0715

. Information found on port submission (587/tcp)


   An SMTP server is running on this port
   Here is its banner :
   220 ESMTP Sendmail 8.11.6+Sun/8.10.2; Wed, 29 Jan 2003
    17:42:18 -0500
    (EST)

. Information found on port unknown (665/tcp)


   This port was detected as being open by a port scanner but is now closed.
   This service might have been crashed by a port scanner or by some
    information gathering plugin

. Vulnerability found on port unknown (898/tcp) :
```

```
    Older versions of JServ (including the version shipped with Oracle9i App
     Server v1.0.2) are vulnerable to a cross site scripting attack using a
     request for a non-existent .JSP file.

    Solution:

    Upgrade to that latest (and final) version of JServ (available at
     java.apache.org), or, for preference use TomCat as JServ is no longer
     maintained.

    Risk factor :
     Medium


 . Warning found on port unknown (898/tcp)


    The remote web server seems to be vulnerable to the Cross Site Scripting
    vulnerability (XSS). The vulnerability is caused by the result returned
    to the user when a non-existing file is requested(e.g. the result
    contains the JavaScript provided in the request).

    The vulnerability would allow an attacker to make the server present the
    user with the attacker's JavaScript/HTML code. Since the content is
    presented by the server, the user will give it the trust
    level of the server (for example, the trust level of banks, shopping
    centers, etc. would usually be high).

    Risk factor : Medium

    Solutions:

    Allaire/Macromedia Jrun:
     http://www.macromedia.com/software/jrun/download/update/
     http://www.securiteam.com/windowsntfocus/Allaire_fixes_Cross-
Site_Scripting_security_vulnerability.html

    Microsoft IIS:
     http://www.securiteam.com/windowsntfocus/IIS_Cross-
Site_scripting_vulnerability__Patch_available_.html

    Apache:
 http://httpd.apache.org/info/css-security/
ColdFusion:
        http://www.macromedia.com/v1/handlers/index.cfm?ID=23047

    General:

      http://www.securiteam.com/exploits/Security_concerns_when_developing_a_
      dynamically_generated_web_site.html
      http://www.cert.org/advisories/CA-2000-02.html



 . Information found on port unknown (898/tcp)
```

```
   A web server is running on this port

. Information found on port unknown (898/tcp)


   The remote web server type is :

   Tomcat/2.1
     Solution : We recommend that you configure (if possible) your web
     server to return a bogus Server header in order to not leak
     information.

. Information found on port unknown (898/tcp)


   The following directories were discovered:
   /help
   /images,
    /servlet


. Information found on port nfs (2049/tcp)


   RPC program #100003 version 2 'nfs' (nfsprog) is running on this
    port

. Information found on port nfs (2049/tcp)


   RPC program #100003 version 3 'nfs' (nfsprog) is running on this
    port

. Information found on port nfs (2049/tcp)


   RPC program #100227 version 2 'nfs_acl' is running on this
    port


. Information found on port nfs (2049/tcp)


   RPC program #100227 version 3 'nfs_acl' is running on this
    port


. Warning found on port nfs (2049/udp)



   The nfsd RPC service is running.
   There is a bug in older versions of
   this service that allow an intruder to
   execute arbitrary commands on your system.
```

```
   Make sure that you have the latest version
   of nfsd

   Risk factor : High
   CVE : CVE-1999-0832

. Information found on port nfs (2049/udp)


   RPC program #100003 version 2 'nfs' (nfsprog) is running on this
    port

. Information found on port nfs (2049/udp)


   RPC program #100003 version 3 'nfs' (nfsprog) is running on this
    port


. Information found on port nfs (2049/udp)


   RPC program #100227 version 2 'nfs_acl' is running on this
    port


. Information found on port nfs (2049/udp)


   RPC program #100227 version 3 'nfs_acl' is running on this
    port


. Information found on port unknown (4045/tcp)


   RPC program #100021 version 1 'nlockmgr' is running on this
    port


. Information found on port unknown (4045/tcp)


   RPC program #100021 version 2 'nlockmgr' is running on this
    port


. Information found on port unknown (4045/tcp)


   RPC program #100021 version 3 'nlockmgr' is running on this
    port


. Information found on port unknown (4045/tcp)
```

```
   RPC program #100021 version 4 'nlockmgr' is running on this
    port

. Warning found on port unknown (4045/udp)



   The nlockmgr RPC service is running.
   If you do not use this service, then
   disable it as it may become a security
   threat in the future, if a vulnerability
   is discovered.

   Risk factor : Low
   CVE : CVE-2000-0508

. Information found on port unknown (4045/udp)


   RPC program #100021 version 1 'nlockmgr' is running on this
    port


. Information found on port unknown (4045/udp)


   RPC program #100021 version 2 'nlockmgr' is running on this
    port


. Information found on port unknown (4045/udp)


   RPC program #100021 version 3 'nlockmgr' is running on this
    port


. Information found on port unknown (4045/udp)


   RPC program #100021 version 4 'nlockmgr' is running on this
    port


. Vulnerability found on port unknown (6112/tcp) :



   The 'dtspcd' service is running.

   Some versions of this daemon are vulnerable to
   a buffer overflow attack which allows an attacker
   to gain root privileges

   *** This warning might be a false positive,
   *** as no real overflow was performed
```

```
   Solution : See http://www.cert.org/advisories/CA-2001-31.html
   to determine if you are vulnerable or deactivate
   this service (comment out the line 'dtspc' in /etc/inetd.conf)

   Risk factor : High
   CVE : CVE-2001-0803

. Vulnerability found on port xfs (7100/tcp) :


   The remote X Font Service (xfs) might be vulnerable to a buffer
   overflow.

   An attacker may use this flaw to gain root on this host
   remotely.

   *** Note that Nessus did not actually check for the flaw
   *** as details about this vulnerability are still unknown

   Solution : See CERT Advisory CA-2002-34
   Risk factor : High
   CVE : CAN-2002-1317

. Vulnerability found on port unknown (8009/tcp) :


   In the default configuration of Oracle9iAS, it is possible to make
   requests for the globals.jsa file for a given web application.
   These files should not be returned by the server as they often
   contain sensitive information.


   Solution:
   Edit httpd.conf to disallow access to *.jsa.

   References:
   http://www.nextgenss.com/advisories/orajsa.txt
   http://www.oracle.com
   Risk factor : Medium/High
   CVE : CAN-2002-0562

. Vulnerability found on port unknown (8009/tcp) :


   In a default installation of Oracle 9iAS, it is possible to access the
   Dynamic Monitoring Services pages anonymously. Access to these pages
   should be restricted.

   Solution:
   Edit httpd.conf to restrict access to /dms0.
   Risk factor :
    High
```

```
. Vulnerability found on port unknown (8009/tcp) :


   In a default installation of Oracle 9iAS it is possible to read the
   Source of JSP files. When a JSP is requested it is compiled 'on the fly'
   and the resulting HTML page is returned to the user. Oracle 9iAS uses a
   folder to hold the intermediate files during compilation. These files are
   created in the same folder in which the .JSP page resides. Hence, it is
   possible to access the .java and compiled .class files for a given JSP
   page.

   Solution:

   Edit httpd.conf to disallow access to the _pages folder.

   References:
   http://wwww.nextgenss.com/advisories/orajsa.txt
   http://www.oracle.com
   Risk factor :
    Medium/High


. Vulnerability found on port unknown (8009/tcp) :


   Older versions of JServ (including the version shipped with Oracle9i App
    Server v1.0.2) are vulnerable to a cross site scripting attack using a
    request for a
   non-existent .JSP file.

   Solution:

   Upgrade to that latest (and final) version of JServ (available at
    java.apache.org), or, for preference use TomCat as JServ is no longer
    maintained.

   Risk factor :
    Medium


. Vulnerability found on port unknown (8009/tcp) :



   The remote host appears to be vulnerable to the Apache
   Web Server Chunk Handling Vulnerability.

   If Safe Checks are enabled, this may be a false positive
   since it is based on the version of Apache.  Although
   unpatched Apache versions 1.2.2 and above, 1.3 through
   1.3.24 and 2.0 through 2.0.36, the remote server may
   be running a patched version of Apache

     *** Note : as safe checks are enabled, Nessus solely relied on the
                banner to issue this  alert

   Solution : Upgrade to version 1.3.26 or 2.0.39 or newer
```

```
   See also : http://httpd.apache.org/info/security_bulletin_20020617.txt
       http://httpd.apache.org/info/security_bulletin_20020620.txt
   Risk factor : High
   CVE : CAN-2002-0392

. Warning found on port unknown (8009/tcp)


   The /doc directory is browsable.
   /doc shows the content of the /usr/doc directory and therefore it shows
    which programs and - important! - the version of the installed programs.

   Solution : Use access restrictions for the /doc directory.
   If you use Apache you might use this in your access.conf:

    <Directory /usr/doc>
    AllowOverride None
    order deny,allow
    deny from all
    allow from localhost
    </Directory>

   Risk factor : High
   CVE : CVE-1999-0678

. Warning found on port unknown (8009/tcp)



   The remote host appears to be running a version of
   Apache which is older than 1.3.27

   There are several flaws in this version, you should
   upgrade to 1.3.27 or newer.

   *** Note that Nessus solely relied on the version number
   *** of the remote server to issue this warning. This might
   *** be a false positive

   Solution : Upgrade to version 1.3.27
   See also : http://www.apache.org/dist/httpd/Announcement.html
   Risk factor : Medium
   CVE : CAN-2002-0840

. Warning found on port unknown (8009/tcp)


   The 'printenv' CGI is installed.
   printenv normally returns all environment variables.

   This gives an attacker valuable information about the
   configuration of your web server.

   Solution : Remove it from /cgi-bin.

   Risk factor : Medium
```

```
. Information found on port unknown (8009/tcp)


   A web server is running on this
    port


. Information found on port unknown (8009/tcp)


   The remote web server type is :

   Oracle HTTP Server Powered by Apache/1.3.19 (Unix) mod_plsql/3.0.9.8.3c
    mod_fastcgi/2.2.10 mod_perl/1.25 mod_oprocmgr/1.0
   Solution : You can set the directive 'ServerTokens Prod' to limit
   the information emanating from the server in its response
    headers.


. Information found on port webcache (8080/tcp)


   A web server is running on this
    port

. Information found on port webcache (8080/tcp)


   The remote web server type is :

   Oracle_Web_listener3.0.2.0.0/2.14FC1
   Solution : We recommend that you configure (if possible) your web server
to
    return
   a bogus Server header in order to not leak information.

. Vulnerability found on port unknown (32771/tcp) :



   The tooltalk RPC service is running.

   There is a format string bug in many versions
   of this service, which allow an attacker to gain
   root remotely.

   In addition to this, several versions of this service
   allow remote attackers to overwrite abitrary memory
   locations with a zero and possibly gain privileges
   via a file descriptor argument in an AUTH_UNIX
   procedure call which is used as a table index by the
   _TT_ISCLOSE procedure.

   *** This warning may be a false positive since the presence
   *** of the bug was not verified locally.

   Solution : Disable this service or patch it
```

```
   See also : CERT Advisories CA-2001-27 and CA-2002-20

   Risk factor : High
   CVE : CAN-2002-0677

. Information found on port unknown (32771/tcp)


   RPC program #100083 version 1 is running on this
    port


. Information found on port unknown (32772/tcp)


   RPC program #300326 version 4 is running on this
    port


. Information found on port unknown (32773/tcp)


   RPC program #100024 version 1 'status' is running on this
    port


. Information found on port unknown (32773/tcp)


   RPC program #100133 version 1 is running on this
    port


. Information found on port general/tcp


   Nmap found that this host is running Sun Solaris 8 early acces beta
through
    actual release

. Warning found on port general/icmp



   The remote host answered to an ICMP_MASKREQ
   query and sent us its netmask (255.255.255.0)

   An attacker can use this information to
   understand how your network is set up
   and how the routing is done. This may
   help him to bypass your filters.

   Solution : reconfigure the remote host so
   that it does not answer to those requests.
   Set up filters that deny ICMP packets of
   type 17.
```

```
   Risk factor : Low
   CVE : CAN-1999-0524

. Warning found on port general/icmp


   The remote host answers to an ICMP timestamp
   request. This allows an attacker to know the
   date which is set on your machine.

   This may help him to defeat all your
   time based authentication protocols.

   Solution : filter out the ICMP timestamp
   requests (13), and the outgoing ICMP
   timestamp replies (14).

   Risk factor : Low
   CVE : CAN-1999-0524

. Vulnerability found on port unknown (32796/udp) :


   The cmsd RPC service is running.
   This service has a long history of
   security holes, so you should really
   know what you are doing if you decide
   to let it run.

   * NO SECURITY HOLE REGARDING THIS
     PROGRAM HAS BEEN TESTED, SO
     THIS MIGHT BE A FALSE POSITIVE *

   We suggest that you disable this
   service.


   Risk factor : High
   CVE : CVE-1999-0320

. Information found on port unknown (32796/udp)


   RPC program #100068 version 2 is running on this
    port


. Information found on port unknown (32796/udp)


   RPC program #100068 version 3 is running on this
    port


. Information found on port unknown (32796/udp)
```

```
   RPC program #100068 version 4 is running on this
    port

. Information found on port unknown (32796/udp)


   RPC program #100068 version 5 is running on this
    port


. Warning found on port unknown (32794/udp)



   The rquotad RPC service is running.
   If you do not use this service, then
   disable it as it may become a security
   threat in the future, if a vulnerability
   is discovered.

   Risk factor : Low
   CVE : CAN-1999-0625

. Information found on port unknown (32794/udp)


   RPC program #100011 version 1 'rquotad' (rquotaprog quota rquota) is
   running on this port


. Warning found on port unknown (32795/udp)



   The rstatd RPC service is running.
   It provides an attacker interesting
   information such as :

    - the CPU usage
    - the system uptime
    - its network usage
    - and more

   Usually, it is not a good idea to let this
   service open


   Risk factor : Low
   CVE : CAN-1999-0624

. Information found on port unknown (32795/udp)


   RPC program #100001 version 2 'rstatd' (rstat rup perfmeter rstat_svc) is
    running on this
```

```
    port

. Information found on port unknown (32795/udp)


   RPC program #100001 version 3 'rstatd' (rstat rup perfmeter rstat_svc) is
    running on this
    port


. Information found on port unknown (32795/udp)


   RPC program #100001 version 4 'rstatd' (rstat rup perfmeter rstat_svc) is
    running on this
    port


. Vulnerability found on port unknown (32793/udp) :



   The sadmin RPC service is running.
   There is a bug in Solaris versions of
   this service that allow an intruder to
   execute arbitrary commands on your system.

   Solution : disable this service
   Risk factor : High
   CVE : CVE-1999-0977

. Information found on port unknown (32793/udp)


   RPC program #100232 version 10 'sadmind' is running on this
    port


. Vulnerability found on port unknown (32799/udp) :



   The remote statd service may be vulnerable
   to a format string attack.

   This means that an attacker may execute arbitrary
   code thanks to a bug in this daemon.

   *** Nessus reports this vulnerability using only
   *** information that was gathered. Use caution
   *** when testing without safe checks enabled.

   Solution : upgrade to the latest version of rpc.statd
   Risk factor : High
   CVE : CVE-2000-0666

. Warning found on port unknown (32799/udp)
```

```
    The statd RPC service is running.
    This service has a long history of
    security holes, so you should really
    know what you are doing if you decide
    to let it run.

    * NO SECURITY HOLES REGARDING THIS
      PROGRAM HAVE BEEN TESTED, SO
      THIS MIGHT BE A FALSE POSITIVE *

    We suggest that you disable this
    service.


    Risk factor : High
    CVE : CVE-1999-0493

 . Information found on port unknown (32799/udp)


    RPC program #100024 version 1 'status' is running on this
     port


 . Information found on port unknown (32799/udp)


    RPC program #100133 version 1 is running on this
     port


 . Information found on port unknown (7937/tcp)


    RPC program #390113 version 1 is running on this
     port


 . Information found on port unknown (32924/udp)


    RPC program #100005 version 1 'mountd' (mount showmount) is running on
this
     port


 . Information found on port unknown (32924/udp)


    RPC program #100005 version 2 'mountd' (mount showmount) is running on
this
     port
```

```
 . Information found on port unknown (32924/udp)


    RPC program #100005 version 3 'mountd' (mount showmount) is running on
this
     port


 . Information found on port unknown (32797/tcp)


    RPC program #100005 version 1 'mountd' (mount showmount) is running on
this
     port


 . Information found on port unknown (32797/tcp)


    RPC program #100005 version 2 'mountd' (mount showmount) is running on
this
     port


 . Information found on port unknown (32797/tcp)


    RPC program #100005 version 3 'mountd' (mount showmount) is running on
this
     port
------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

Appendix B - CIS Scan Results

*** CIS Ruler Run ***
Starting at time 20030125-14:26:47

Negative: 1.1 System appears not to have been patched within the last month.
Negative: 2.2 telnet not deactivated.
Negative: 2.3 ftp not deactivated.
Negative: 2.4 rsh (shell) should be deactivated.
Positive: 2.5 tftp is deactivated.
Positive: 2.6 network printing is deactivated.
Negative: 2.7 rquotad is not deactivated.
Negative: 2.8 CDE-related daemon rpc.ttdbserverd not deactivated in inetd.conf.
Negative: 2.8 CDE-related daemon fs.auto (port fs) not deactivated in inetd.conf.
Negative: 2.10 kerberos net daemon ktkt_warnd not deactivated in inetd.conf.
Negative: 2.10 kerberos net daemon gssd not deactivated in inetd.conf.
Negative: 3.1 llc2 not deactivated.
Negative: 3.1 uucp not deactivated.
Negative: 3.1 slpd not deactivated.
Negative: 3.1 flashprom not deactivated.
Negative: 3.1 PRESERVE not deactivated.
Negative: 3.1 bdconfig not deactivated.
Negative: 3.1 wbem not deactivated.
Negative: 3.1 ncalogd not deactivated.
Negative: 3.1 ncad not deactivated.
Negative: 3.1 mipagent not deactivated.
Negative: 3.1 sysid.net not deactivated.
Negative: 3.1 sysid.sys not deactivated.
Negative: 3.1 autoinstall not deactivated.
Negative: 3.1 asppp not deactivated.
Negative: 3.1 cachefs.daemon not deactivated.
Negative: 3.1 cacheos.finish not deactivated.
Negative: 3.1 power not deactivated.
Negative: 3.3 NFS Server script nfs.server not deactivated.
Negative: 3.4 NFS script nfs.client not deactivated.
Negative: 3.4 NFS script autofs not deactivated.
Negative: 3.5 rpc rc-script (rpcbind) not deactivated.
Negative: 3.8 ldap cache manager not deactivated.
Negative: 3.9 lp not deactivated.
Negative: 3.9 spc not deactivated.
Negative: 3.10 volume manager not deactivated.
Negative: 3.11 Graphics adaptor initialization script afbinit not deactivated.
Negative: 3.11 Graphics adaptor initialization script ifbinit not deactivated.
Negative: 3.12 Mail daemon is on and collecting mail from the network.
Negative: 3.13 Apache web server rc-script not deactivated.
Positive: 3.14 snmp daemon is deactivated.
Positive: 3.16 syslogd has the -t switch and is thus not listening to the network.
Negative: 3.17 inetd is still active.
Negative: 3.18 Serial login prompt not disabled.
Positive: 3.19 Found a good daemon umask of 022 in /etc/default/init.
Negative: 4.1 Coredumps aren't deactivated.
Positive: 4.2 Stack is set non-executable
Negative: 4.3 NFS clients aren't restricted to privileged ports.
Negative: 4.4 tcp_ip_abort_cinterval should be at most 60,000 to avoid TCP flood problems.
Positive: 4.5 Network parameters are set well.

Positive: 4.6 TCP sequence numbers strong enough.
Positive: 5.1 syslog captures auth messages.
Negative: 5.2 syslog does not permanently capture daemon.debug messages.
Negative: 5.2 ftp is running out of inetd on port ftp, but does not do "-d" debug logging.
Negative: 5.3 /var/adm/loginlog doesn't exist to track failed logins.
Positive: 5.4 cron usage is being logged.
Positive: 5.5 System accounting appears to be enabled.
Positive: 5.6 kernel-level auditing is enabled and flags meet or exceed minimum values.
Negative: 5.7 /var/adm/wtmpx should not be world or group writable.
Negative: 6.1 /usr is not mounted read-only.
Negative: 6.1 /orafs01 is not mounted nosuid.
Negative: 6.1 /orafs20 is not mounted nosuid.
Negative: 6.1 /orafs02 is not mounted nosuid.
Negative: 6.1 /orahotback is not mounted nosuid.
Negative: 6.1 /orafs21 is not mounted nosuid.
Negative: 6.1 /orafs03 is not mounted nosuid.
Negative: 6.1 /aps11ip is not mounted nosuid.
Negative: 6.1 /orafs22 is not mounted nosuid.
Negative: 6.1 /orafs04 is not mounted nosuid.
Negative: 6.1 /orafs05 is not mounted nosuid.
Negative: 6.1 /orafs06 is not mounted nosuid.
Negative: 6.1 /orafs07 is not mounted nosuid.
Negative: 6.1 /orafs08 is not mounted nosuid.
Negative: 6.1 /orafs09 is not mounted nosuid.
Negative: 6.1 /orafs10 is not mounted nosuid.
Negative: 6.1 /orafs11 is not mounted nosuid.
Negative: 6.1 /orafs12 is not mounted nosuid.
Negative: 6.1 /orafs13 is not mounted nosuid.
Negative: 6.1 /orafs14 is not mounted nosuid.
Negative: 6.1 /orafs15 is not mounted nosuid.
Negative: 6.1 /archive is not mounted nosuid.
Negative: 6.1 /orafs16 is not mounted nosuid.
Negative: 6.1 /orafs17 is not mounted nosuid.
Negative: 6.1 /orafs18 is not mounted nosuid.
Negative: 6.1 /orafs19 is not mounted nosuid.
Negative: 6.1 /var is not mounted nosuid.
Negative: 6.1 /home is not mounted nosuid.
Negative: 6.1 /dbadmin is not mounted nosuid.
Positive: 6.2 logging option is set on root file system
Positive: 6.3 /etc/rmmount.conf mounts all file systems nosuid.
Positive: 6.4 /etc/dfs/dfstab doesn't have any non-fully qualified pathname share commands.
Negative: 6.5 /etc/shadow is not owned by group sys!
Positive: 6.6 all temporary directories have sticky bits set.
Negative: 7.1 /etc/pam.conf appears to support rhost auth.
Positive: 7.2 /etc/hosts.equiv and root's .rhosts/.shosts files either don't exist or are links to /dev/null.
Positive: 7.3 All users necessary are present in /etc/ftpusers
Positive: 7.4 /etc/shells exists and has good permissions.
Negative: 7.7 /etc/dt/config/en_US.UTF-8/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 7.7 /etc/dt/config/C/sys.resources doesn't exist, so screenlocker can't be set.
Negative: 7.8 Couldn't open cron.allow
Negative: 7.8 Couldn't open at.allow
Positive: 7.11 Root is only allowed to login on console
Positive: 7.12 /etc/default/login allows 2 login attempts.
Negative: 7.13 EEPROM isn't password-protected.
Negative: 7.13 EEPROM failed logins aren't logged.
Positive: 8.1 All system accounts are locked/deleted.

Negative: 8.2 User sdali should have a minimum password life of at least 7 days.
Negative: 8.2 User alincoln should have a minimum password life of at least 7 days.
Negative: 8.2 User cgrant should have a minimum password life of at least 7 days.
Negative: 8.2 User owilde should have a minimum password life of at least 7 days.
Negative: 8.2 User rwagner should have a minimum password life of at least 7 days.
Negative: 8.2 User jstark should have a minimum password life of at least 7 days.
Negative: 8.2 User mbishop should have a minimum password life of at least 7 days.
Negative: 8.2 User rmorris should have a minimum password life of at least 7 days.
Negative: 8.2 User oracle should have a minimum password life of at least 7 days.
Negative: 8.2 User oracle should have a maximum password life of between 1 and 91 days.
Negative: 8.2 User oracle should have a password expiration warning of at least 7 days.
Negative: 8.2 User jkirk should have a minimum password life of at least 7 days.
Negative: 8.2 User vputin should have a minimum password life of at least 7 days.
Negative: 8.2 /etc/default/passwd doesn't have a value for MAXWEEKS.
Negative: 8.2 /etc/default/passwd doesn't have a value for MINWEEKS.
Negative: 8.2 /etc/default/passwd doesn't have a value for WARNWEEKS.
Positive: 8.3 There were no +: entries in passwd, shadow or group maps.
Positive: 8.4 All users have passwords
Positive: 8.5 Only one UID 0 account AND it is named root.
Positive: 8.6 root's PATH is clean of group/world writable directories or the current-directory link.
Negative: 8.7 User sdali has a world-readable homedir!
Negative: 8.7 User alincoln has a world-executable homedir!
Negative: 8.7 User cgrant has a world-executable homedir!
Negative: 8.7 User owilde has a world-executable homedir!
Negative: 8.7 User owilde has a world-readable homedir!
Negative: 8.7 User rwagner has a world-executable homedir!
Negative: 8.7 User jstark has a world-executable homedir!
Negative: 8.7 User mbishop has a world-executable homedir!
Negative: 8.7 User rmorris has a world-executable homedir!
Negative: 8.7 User oracle has a world-executable homedir!
Negative: 8.7 User jkirk has a world-executable homedir!
Negative: 8.7 User ias has a world-executable homedir!
Negative: 8.7 User vputin has a world-executable homedir!
Negative: 8.7 User byeltsin has a world-executable homedir!
Negative: 8.7 User lwall has a world-executable homedir!
Negative: 8.10 Default umask (000) may not block world-read/write/execute. Check /etc/default/login.
Negative: 8.10 Default umask (000) may not block group-read/write/execute. Check /etc/default/login.
Negative: 8.10 Default umask (000) may not block world-read/write/execute. Check /etc/.login.
Negative: 8.10 Default umask (000) may not block group-read/write/execute. Check /etc/.login.
Negative: 8.11 /etc/profile should have mesg n to block talk/write commands and strengthen permissions on user tty.
Negative: 8.11 /etc/.login should have mesg n to block talk/write commands and strengthen permissions on user tty.
Negative: 9.1 tcp-protocol service fs in inetd.conf is not wrapped.
Negative: 9.1 tcp-protocol service opirpc in inetd.conf is not wrapped.
Negative: 9.1 tcp-protocol service opirpc8 in inetd.conf is not wrapped.
Negative: 9.1 tcp-protocol service dtspc in inetd.conf is not wrapped.
Negative: 9.1 tcp6-protocol service sun-dr in inetd.conf is not wrapped.
Positive: 9.2 System is running sshd.
Negative: 9.3 Fix-modes has not been run here.
Preliminary rating given at time: Sat Jan 25 14:26:49 2003

Preliminary rating = 5.57 / 10.00

Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edJobRenameForm.jsp

Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/download.sh
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_hu.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_VE.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/asynch_job.trg
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/admin/LocationMark.properties
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_en_ZA.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_en_IE_EURO.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/smvall.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_tr.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/warning.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/hook/MyFolderRendererContext.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/editJob_r.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edJobOutParamForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/rc02ur.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/DoLogin.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/spatial/router/Routers.xml
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/userService.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tplusr.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_no_NO_NY.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/doJobCreate.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/create_aq_new.bat
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/LoadRMData.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/doBookmarkCreate.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/warnl.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/spatial/mapper/Mappers.xml
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/srmvall.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/EdLandmark.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/serviceTitleBar.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/localClose.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_th.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_CL.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edBookmarkContent.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/doFolderMove.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/phone_right.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tplus.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edPasswordChangeForm.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/router/Sample102TextRouter.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edBookmarkCreateForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/topBar.jsp

Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edBookmarkSubmitForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/folderclosed.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edBookmarkChangeForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/loadRMData.sh
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/DeployServiceFolder.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_fr_BE_EURO.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_zh_TW.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/mod_header_right_corner.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_el_GR.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edFolderListForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_nl_NL_EURO.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edServiceResource.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/doAgentSucc.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/insService.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tline.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_cs_CZ.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/CreateURLService.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/sampleadapter/spatial/mapper/SampleBusinessCategoryMapper.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edAgentSelectForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_SV.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_pt_PT.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/classes/oracle/panama/core/admin/Provisioning.properties
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_fr_FR_EURO.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/doServiceRename.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/sampleadapter/spatial/router/SampleTextRouter.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edUserPrefSubmitForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edAgentEditForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/login_ena.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/upgrade_inst.sh
Negative: 6.7 Non-standard world-writable file: /ias/panama/setupconf/param.sh
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/constants.pkg
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/folder_12x11.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/runMasterServer.bat
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/PhoneLeft.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/classes/oracle/panama/spatial/yp/YPCategoriesVicinity.xml

Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_it_IT.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_hr_HR.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edAgentCreateForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/setupconf/pa_java_inst_upgrade.sh
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_it.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/service.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_ES.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/setEncoding.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/select_upper.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/router/SampleRouterI.java
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/spatial/yp/YPCategories.xml
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/panama/mp/MPSample.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/ShowError.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/listener/RequestListenerSample.class
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ca.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_PR.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tfold.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/smalledit.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/folder_expand.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/create_all.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/hook/SessionIdSample.java
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_MX.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/homeImage.jpg
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/adv2.gif
Negative: 6.7 Non-standard world-writable file: /ias/otrace/admin/facility.dat
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_de_AT.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/xform/xsl/PLAIN_TEXT.xsl
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/insFolder.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/Sample102BaseAdapter.class
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/admin/EncodingSets.properties
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/admin/Cookies.properties
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/doJobSetUp.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_en_NZ.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/doServiceSaveParam.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edFolderAddForm.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_sv_SE.js

Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edServiceTitleBar.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_sk.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_en_IE.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_BO.js
Negative: 6.7 Non-standard world-writable file: /ias/patches/2424256/Disk1/stage/Components/oracle.swd.jre/1.1.8.10a/1/DataFiles/Expanded/jre/solaris/bin/jre
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/RunService.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edServiceContentForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/sampleadapter/spatial/yp/Sample102BusinessNameSearch.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_en_AU.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/bookmark.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/create_aq_user.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/sampleadapter/spatial/router/Sample102Router.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/classes/oracle/panama/adapter/ldap/ldap.properties
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_fr_CA.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tleafb.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/doAgentChange.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tnavnd.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/sampleadapter/spatial/geocoder/Sample102Geocoder.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/blueball.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/adminLoginError.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/classes/oracle/panama/spatial/spatial.properties.templ
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/styles/blaf.xss
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edPrefInputs.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/sampleadapter/spatial/Sample102BaseAdapter.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_sh_YU.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edFolderMenuImage.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_zh.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/classes/oracle/panama/adapter/papzlite/LocalStrings.properties
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/sampleadapter/spatial/mapper/Sample102BusinessNameMapper.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_HN.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/sampleadapter/HelloWorld.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/listener/ResponseListenerSample.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edServiceIns.jsp

Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/doAgentEdit.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/whitestripestop.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_pt_BR.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/MyLandmark.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/xml/XMLXSL.properties
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/upgrade_inst.bat
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_sv.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ar_SD.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/editJob_s.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/drop_all.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/adv.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/errorA.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/PapzError.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/DateField.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/editContent_r.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/setupconf/pa_java.sh
Negative: 6.7 Non-standard world-writable file: /ias/6iserver/otrace/admin/facility.dat
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_et_EE.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/confl.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/radiods.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/userPref_r.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/doFolderContent.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/getServiceTitle.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/util/client/xmleditor/images/expanded.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tleafr.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/userServiceLarge.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ca_ES.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/smvuptop.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ko_KR.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ar_SY.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tleaf.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_uk_UA.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_sl.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_AR.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/doJobMove.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/treeElementRenderer.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/WEB-INF/jsp/TreeFunc.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tnavp.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_fi_FI.js

Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/xform/xsl/HDML.xsl
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/close.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/login.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/editJob_n.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_de_DE.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/DoBookmark.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/small_logo.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/telcoServiceLarge.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/hook/MyAuthenticationModule.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/TestService.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/editServiceDialog.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/disable_cachesync_triggers.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/radiodn.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tsb.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/whitecorners.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edFolderContTitle.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/encryptPassword.bat
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_nl.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_nl_BE_EURO.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/create.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/doJobCreateErrChk.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/loginError.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/addBookmark_r.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/job_filter_r.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/adminUserLogin.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/probe/www-server.properties
Negative: 6.7 Non-standard world-writable file: /ias/6iserver/otrace/admin/regid.dat
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/iaswe_logo_large.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/spacer.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_da.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/doJobRename.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/listener/ListenerRegistrationHookSample.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/aq_drop.sql
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_be.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/index.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/DoRegisterSelf.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/checkrc.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/WMLPatternFormat.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/magent/config/MAgent.properties
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ar_OM.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/loginForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/adv3.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/upload.sh

Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edServiceError.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/EdAlert.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/logout_r.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/spatial/region/RMException.properties
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/DoTestService.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/magent_schema.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/editFolderDialog.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/AdEdGroupService.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/adapter/xsl/sql2panama.xsl
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/aq_object.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/model/SampleModelAdapter.class
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_de_LU.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edServiceMenu.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_fr.js
Negative: 6.7 Non-standard world-writable file: /ias/otrace/admin/collect.dat
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_et.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/folder_collapse.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_CO.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/AdAssignGroup.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/router/Sample102TextRouter.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/logon_header.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ro.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ar_BH.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/DoDeployServiceOwner.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/sys_logger_schema.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edUserPrefError.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/insBookmark.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edFolderContListF.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/mp/positioner.xml
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/papz.css
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/yp/SampleBusinessCategorySearch.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/ShowWarning.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/insJob.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/addService_r.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/smvup.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_de_CH.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edBookmarkInputs.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/mapper/Sample102BusinessCategoryMapper.java
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_tr_TR.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/blank.gif

Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/info.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ru_RU.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/RegisterSelf.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/folderContent.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edServiceHeader.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_fr_BE.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ar_TN.js
Negative: 6.7 Non-standard world-writable file: /ias/6iserver/otrace/admin/collect.dat
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edFolder.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_mk_MK.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/samples.xml
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/master/Master.properties
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ar.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/DoAlert.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/mapper/SampleMapper.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/extattr.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/finish.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edAgentCreateError.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/whitestripes.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/WEB-INF/jsp/PageTemp.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/GeocoderNew.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/setupconf/sqlnet.ora
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_pt_PT_EURO.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/job_r.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/localClose.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/AdCreateUser.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_fr_FR.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/mapper/SampleBusinessNameMapper.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/finishedButton.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/cancel.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/bullet.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_iw.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/MyAlertAddress.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsps/calendarDialog.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edJobMoveForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/addFolder_r.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/doJobChangeErrChk.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/spatial/geocoder/Geocoders.xml
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/AdDoAllGroup.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edFolderMenu.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/hook/MyAuthenticationModule.java

Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/sampleadapter/HelloAdapter.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edServiceInputs.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edFolderContent.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/DoLandmark.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/editJobDialog.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/drop_sys_logger_schema.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/editContent_s.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/telcoFolder.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/AdEdGroupRoot.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/checkrn.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/warningA.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/userPref_s.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/getUserPrefTitle.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/doBookmarkCreateErrChk.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/WEB-INF/jsp/Constant.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/classes/oracle/panama/core/admin/System.properties.templ
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/hook/MyFolderRendererContext.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/sampleadapter/spatial/mapper/SampleMapper.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/enable_cachesync_triggers.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/getJobTitle.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/classes/oracle/panama/adapter/stripper/Strip.properties
Negative: 6.7 Non-standard world-writable file: /ias/patches/2424256/Disk1/stage/Components/oracle.swd.jre/1.1.8.10a/1/DataFiles/Expanded/jre/solaris/bin/sparc/native_threads/jre
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/home.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/up102-11.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edServiceParamForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/AdDoCreateUser.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_pt.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/doFolderAction.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/required.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/srmv.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/sampleadapter/spatial/SampleBaseAdapter.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/folder.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/classes/oracle/panama/core/admin/Notification.properties
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/errorl.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/deleteAgent_r.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/serviceDisplay.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/greetings.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ar_YE.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edUserPrefMenu.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ja.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edFolderMoveForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/editContent_n.gif

Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/object.sql
Negative: 6.7 Non-standard world-writable file: /ias/Apache/Jserv/logs/jserv_old.log
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/MyAlert.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/horizontal_white_line.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/folderTitleBar.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/hook/MyFolderRenderer.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/create_spatial.sql
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/mapper/Sample102BusinessNameMapper.java
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_fi.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ar_DZ.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/userPref_n.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/listener/ResponseListenerSample.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/insUserPref.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/setupconf/tnsnames.ora
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/admin/persistent.properties
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/smalleredit.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/hook/MyAuthenticator.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/bluestripestop.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/admin/AsynchRequest.properties
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_PA.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_en_GB.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_be_BY.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/addBookmark_s.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/job_filter_s.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/AdDoGroupService.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/spatial/yp/YPProviders.xml
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_ES_EURO.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/doAgentAction.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/Locale.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/doServiceAction.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/styles/blaf.css
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/object.trg
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/yp/Sample102BusinessNameSearch.java
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/adapter/mail/MailAdapter.properties
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_sk_SK.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_bg.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/download.bat
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_pl_PL.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/adv4.gif

Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/images/smvdownbottom.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/AdDoGroupRoot.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_no_NO.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/logout_s.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/password_r.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ar_KW.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tminusf.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/mapper/SampleBusinessCategoryMapper.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/WEB-INF/jsp/UtilFunc.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/folderRenderer.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/AdDoAllUser.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_is_IS.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edServiceContent.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/addBookmark_n.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/job_filter_n.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/admin/System.properties
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edAgentModForm.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_uk.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_DO.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/admin/Rmi.properties
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tminusaf.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edPrefResource.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/router/SampleRouterI.class
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_fr_LU_EURO.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edServiceCreateForm.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/spatial/region/RMSuggestion.properties
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edServiceSubmitForm.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/spatial/spatial.properties
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ar_QA.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/loadRMData.bat
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/phone_left.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/doServiceMove.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/xform/xsl/VoiceXML.xsl
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/DoCreateURLService.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/addService_s.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_de_AT_EURO.js

Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ja_JP.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tplusaf.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ar_JO.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ar_IQ.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/sampleadapter/HelloWorld.java
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/yp/Sample102BusinessCategorySearch.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/logout_n.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edFolderSubmitForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/setupconf/pa_java_inst.bat
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_EC.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/DeployServiceOwner.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tminusa.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_el.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/widls/onlineQuoteYahoo.widl
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/papz.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/service.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/topBar.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_fi_FI_EURO.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_no.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/newfolder_16x15.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/dsort.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/job_s.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/yp/SampleBusinessNameSearch.class
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/mapper/Sample102BusinessCategoryMapper.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/addService_n.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_GT.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/addFolder_s.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/move_r.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edJobSubmitForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/model/SampleModelAdapter.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/logout.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/headerStripes.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/curve.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/doJobChange.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edJobChangeForm.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/yp/SampleBusinessNameSearch.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/doAgentErrChk.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/treeView.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/create_views.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/doBookmarkChange.jsp

Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edJobResource.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/telcoFolderLarge.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/doAgentCreate.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_en_CA.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_zh_HK.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/doAdminUserLogin.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/doPasswordChange.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/commands.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/panama.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/PasswordHint.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edJob.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/drop_spatial.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edBookmarkMenu.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/job_n.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/listener/SessionListenerSample.class
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/router/SampleTextRouter.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/panama/mp/MPSample.class
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_CR.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/addFolder_n.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/xform/xsl/MML.xsl
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/topBackground.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/iaswe_logo.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/adapter/ldap/LocalStrings.properties
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/phone_top.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_th_TH.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/up11-111.xml
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/deleteAgent_s.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/router/Sample102Router.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/toolbarBG.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/doFolderRename.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/t.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/ShowService.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edFolderError.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/PapzMain.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edJobContent.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/geocoder/SampleGeocoder.java
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_lt_LT.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/drop_views.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edFolderResource.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/panamaLogo.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_pl.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/radiors.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edJobInputs.jsp

Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ar_LB.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_lt.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/help_r.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/geocoder/SampleGeocoder.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/create_aq.sh
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/defaultAgent_r.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/WEB-INF/jsp/ServiceFunc.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/deleteAgent_n.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/editUserFolder_r.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_bg_BG.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/adapter/mail/LocalStrings.properties
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/spatial/yp/YPCategoriesInfoUSA.xml
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/infoA.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/rename_r.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_de.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/xform/xsl/CHTML.xsl
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/userFolderLarge.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/initPRequest.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_de_DE_EURO.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/password_s.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/ok.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/getFolderTitle.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/hook/MyFolderRenderer.java
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/admin/AsynchNotification.properties
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/login_logo.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/xform/xsl/TINY_HTML.xsl
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_hr.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/radiorn.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tleafbf.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/smv.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/doJobAction.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_sq.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/parm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edAgentContent.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/createAgent_r.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tplusf.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/doBookmarkAction.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edBookmark.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/RegExpFormat.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/yp/SampleBusinessCategorySearch.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/WEB-INF/jsp/InitRequest.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edFolderIns.jsp

Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_iw_IL.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/editAgent_r.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/migrate_8i_to_9i.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsps/frameRedirect.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/password_n.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/AdAllUser.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_UY.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/magent/config/MInstances.properties
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tminusb.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/util/client/xmleditor/images/folder.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/admin/Ftp.properties
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_en.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/datePicker.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/AdDoGroup.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/copy_r.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/folderImage.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/upload.bat
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/create_aq.bat
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edPasswordChangeError.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ar_MA.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tplusa.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/SampleBaseAdapter.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/hook/MyAuthenticator.java
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/admin/UserAgents.properties
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tip.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/move_s.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_sl_SI.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/powered_by.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_it_CH.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/folderopen.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/portallogo.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/DoFolder.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/TableProxy.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/PhoneTop.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_PY.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/AdAllGroup.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_en_US.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/loginAuthenticate.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_nl_NL.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/logout_ena.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edServiceFooter.jsp

Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_lv_LV.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/admin/ProxyFirewall.properties
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/doServiceCreate.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tnavpd.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/adapter/xsl/sql2panama_ar.xsl
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/drop.sql
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_hu_HU.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/doAgentModErrChk.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tminusr.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/xform/xsl/WML11.xsl
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ar_EG.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/MyService.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/move_n.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_sr.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/admin/Oemevent.properties
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/DateFormat.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/select_lower.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/classes/oracle/panama/core/admin/LocationMark_en_US.properties
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_nl_BE.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/buttonedit.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/mapper/SampleBusinessNameMapper.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/queue.pkg
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/help_ena.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_fr_LU.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/edit.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/upgrade_inst.txt
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/copyfolder.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/create_cachesync_schema.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edFolderContListS.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edJobMenu.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/userFolder.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/runMasterServer.sh
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/papz/images/mod_header_left_corner.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/geocoder/Sample102Geocoder.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tminusbf.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_fr_CH.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/Shuttle.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/portal.js

Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/userPrefDialog.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/mainError.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/Login.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_sh.js
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_cs.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edUserPref.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/DoService.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_PE.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edAgentInputs.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ar_AE.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-
INF/jsp/edServiceMoveForm.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_es_NI.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tplusbf.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tnavn.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/checkdc.gif
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_lv.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/help_s.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/DecimalFormat.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/rc02ul.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/defaultAgent_s.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/DoMyService.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/bootstrap.xml
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/editUserFolder_s.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/WEB-INF/jsp/HookFunc.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/encryptPassword.sh
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/newtoolbar.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/DoMyAlert.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/rename_s.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edUserPrefContent.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/PhoneRight.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/listener/RequestListenerSample.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/error.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/EdBookmark.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/folderDisplay.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tminus.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/aq_grants.sql
Negative: 6.7 Non-standard world-writable file:
/ias/panama/sample/sampleadapter/spatial/yp/Sample102BusinessCategorySearch.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/setImageDir.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ar_LY.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/mainView.jsp
Negative: 6.7 Non-standard world-writable file:
/ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_de_LU_EURO.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/DoDeployServiceFolder.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/smvdown.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/edService.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/sql/up11-111.sql
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/PhoneBottom.jsp

Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edFolderContentForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/EdService.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/MyProfile.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/DoMyAlertAddress.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/help_n.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edJobForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/defaultAgent_n.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/getEditLogicalDevice.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/phone_bottom.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ar_SA.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/adminLoginForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/oldservice.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/editUserFolder_n.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ru.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/infol.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/createAgent_s.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/classes/oracle/panama/util/client/xmleditor/images/collapsed.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/sampleadapter/HelloAdapter.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/rename_n.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tminusrf.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/hook/SessionIdSample.class
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_it_IT_EURO.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/asort.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ro_RO.js
Negative: 6.7 Non-standard world-writable file: /ias/otrace/admin/regid.dat
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/doPassErrChk.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/getLogicalDevice.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/test.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/login.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_da_DK.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_sr_YU.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tleaff.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/editAgent_s.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/portal.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/LoadRMData.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tplusrf.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/WEB-INF/jsp/CleanRequest.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/EdFolder.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_zh_CN.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/show.gif
Negative: 6.7 Non-standard world-writable file: /ias/6iserver/discwb4/bin/regentry
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edServiceRenameForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edFolderInputs.jsp

Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/copy_s.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/DoLogout.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/close_g.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/MarlinCore.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/doJobOutParam.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/js.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/DoMyLandmark.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/createAgent_n.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/DoMyProfile.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/tplusb.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/telcoService.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/edFolderRenameForm.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/portal1.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/images/checkdn.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/classes/oracle/panama/webui/LocalStrings.properties
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/listener/ListenerRegistrationHookSample.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/editAgent_n.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/sample/listener/SessionListenerSample.java
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/images/webptglogo.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/WEB-INF/jsp/doFolderAdd.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/Home.jsp
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_mk.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/papz/images/copy_n.gif
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_sq_AL.js
Negative: 6.7 Non-standard world-writable file: /ias/panama/server/portal/cabo/jsLibs/resources/LocaleElements_ko.js
Negative: 6.8 Non-standard SUID program /oracle/products/V920/bin/oracleO
Negative: 6.8 Non-standard SUID program /oracle/V920/bin/oracle
Negative: 6.8 Non-standard SUID program /oracle/V920/bin/oradism.sav
Negative: 6.8 Non-standard SUID program /oracle/V920/dbs/orapwmrsp
Negative: 6.8 Non-standard SUID program /oracle/V920/bin/oradism
Negative: 6.8 Non-standard SUID program /ias/bin/oracle
Negative: 6.8 Non-standard SUID program /usr/local/libexec/ssh-keysign
Negative: 6.8 Non-standard SUID program /opt/ORCLfmap/bin/fmputl
Negative: 6.8 Non-standard SUID program /oracle/V920/dbs/orapwissntlog
Negative: 6.8 Non-standard SUID program /oracle/V920/bin/dbsnmp
Negative: 6.8 Non-standard SUID program /usr/local/bin/sudo
Negative: 6.8 Non-standard SGID program /ias/bin/dbsnmp
Negative: 6.8 Non-standard SGID program /oracle/V920/bin/oracleO
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/admgroupls
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/admgroupmod
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/hostmgr
Negative: 6.8 Non-standard SGID program /oracle/V920/bin/oradism
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/usermgr
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/admhostdel
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/admuserdel
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/admgroupadd
Negative: 6.8 Non-standard SGID program /oracle/V920/bin/oracle
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/admhostmod
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/admusermod

Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/admtblloc
Negative: 6.8 Non-standard SGID program /home/sdali/top
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/admhostadd
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/admuseradd
Negative: 6.8 Non-standard SGID program /applications2/iasapps/bin/oracleO
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/stomgr
Negative: 6.8 Non-standard SGID program /oracle/V920/bin/oradism.sav
Negative: 6.8 Non-standard SGID program /usr/local/bin/lsof
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/serialmgr
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/admserialdel
Negative: 6.8 Non-standard SGID program /ias/bin/oracle
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/dbmgr
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/admserialmod
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/groupmgr
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/admupgrade
Negative: 6.8 Non-standard SGID program /usr/local/bin/top
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/admuserls
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/admserialls
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/printmgr
Negative: 6.8 Non-standard SGID program /oracle/V920/bin/dbsnmp
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/admreboot
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/admhostls
Negative: 6.8 Non-standard SGID program /opt/SUNWadm/2.3/bin/admgroupdel
Ending run at time: Sat Jan 25 15:01:30 2003

Final rating = 3.57 / 10.00

Appendix C - Patchdiag Output

```
================================================================================
System Name: roarke     SunOS Vers: 5.8         Arch: sparc
Cross Reference File Date: Jan/30/03

PatchDiag Version: 1.0.4
================================================================================
Report Note:

Recommended patches are considered the most important and highly
recommended patches that avoid the most critical system, user, or
security related bugs which have been reported and fixed to date.
A patch not listed on the recommended list does not imply that it
should not be used if needed.  Some patches listed in this report
may have certain platform specific or application specific dependencies
and thus may not be applicable to your system.  It is important to
carefully review the README file of each patch to fully determine
the applicability of any patch with your system.
================================================================================
INSTALLED PATCHES
Patch  Installed Latest   Synopsis
  ID   Revision  Revision
------ --------- -------- ------------------------------------------------------
108434    08        10    32-Bit Shared library patch for C++
108435    08        10    64-Bit Shared library patch for C++
108528    15        18    SunOS 5.8: kernel update patch
108569    04        08    X11 6.4.1: platform support for new hardware
108576    11        33    SunOS 5.8: Expert3D IFB Graphics Patch
108604    14        31    SunOS 5.8: Elite3D AFB Graphics Patch
108605    12        32    SunOS 5.8: Creator and Creator3D: FFB Graphics Patch
108606    08        29    SunOS 5.8:  M64 Graphics Patch
108609    01     CURRENT  SunOS 5.8: Buttons/Dials Patch
108623    02        03    SunOS 5.8: Thai Wordbreak Iterator module
108652    56        64    X11 6.4.1: Xsun patch
108664    07     CURRENT  Obsoleted by: 112137-01 SunOS 5.8: Support for Network Service Pro
108680    09     CURRENT  Obsoleted by: 111041-01 SunOS 5.8: su, su_pnp, and eri driver patc
108714    05        07    CDE 1.4: libDtWidget patch
108723    01     CURRENT  SunOS 5.8: /kernel/fs/lofs and /kernel/fs/sparcv9/lofs patch
108725    11        12    SunOS 5.8: st driver patch
108727    16        19    SunOS 5.8: /kernel/fs/nfs and /kernel/fs/sparcv9/nfs patch
108773    08        17    SunOS 5.8: IIIM and X Input & Output Method patch
108806    12        14    SunOS 5.8: Sun Quad FastEthernet qfe driver
108808    23        42    SunOS 5.8: Manual Page updates for Solaris 8
108813    05        11    SunOS 5.8: Sun Gigabit Ethernet 3.0
108820    01     CURRENT  SunOS 5.8: nss_compat.so.1 patch
108823    01     CURRENT  SunOS 5.8: compress/uncompress/zcat patch
108825    01     CURRENT  Obsoleted by: 110896-02 SunOS 5.8: /usr/lib/fs/cachefs/cfsadmin pa
108827    26        38    SunOS 5.8: /usr/lib/libthread.so.1 patch
108833    04        05    Obsoleted by: 111498-04 SunOS 5.8: kdmouse and kb_ps2 driver patch
108835    02        03    CDE 1.4: dtcm patch
108869    18     CURRENT  SunOS 5.8: snmpdx/mibiisa/libssasnmp/snmplib patch
108875    12        13    SunOS 5.8: c2audit patch
108897    01     CURRENT  X11 6.4.1 Xprint patch
108899    01        03    SunOS 5.8: /usr/bin/ftp patch
108901    05        06    SunOS 5.8: /kernel/sys/rpcmod and /kernel/strmod/rpcmod patch
108909    09        12    CDE 1.4: Smart Card Administration GUI patch
108914    02     CURRENT  SunOS 5.8: l10n update: PDA Sync, SmartCard, DHCP mgr, Printer Adm
108919    15     CURRENT  CDE 1.4: dtlogin patch
108921    11        16    CDE 1.4: dtwm patch
108923    01     CURRENT  CDE 1.4: dtwm audio control patch
108940    16        49    Motif 1.2.7 and 2.1.1: Runtime library patch for Solaris 8
108947    01     CURRENT  Obsoleted by: 108528-13 SunOS 5.8: /platform/sun4u/cprboot patch
108949    07     CURRENT  CDE 1.4: libDtHelp/libDtSvc patch
108954    02     CURRENT  SunOS 5.8: localization updates for different components
108962    01     CURRENT  SunOS 5.8: XmlReader fails on an HTTP stream
108964    04        06    SunOS 5.8: /usr/sbin/in.tftpd and /usr/sbin/snoop patch
108968    07        08    SunOS 5.8: vol/vold/rmmount/dev_pcmem.so.1 patch
108970    01     CURRENT  SunOS 5.8: /usr/lib/fs/pcfs/fsck and /usr/lib/fs/pcfs/mkfs patch
108972    04     CURRENT  SunOS 5.8: /sbin/fdisk patch
108974    21        25    SunOS 5.8: dada, uata, dad, sd and scsi drivers patch
108975    06     CURRENT  SunOS 5.8: /usr/bin/rmformat and /usr/sbin/format patch
108977    01     CURRENT  SunOS 5.8: libsmedia patch
108981    08        10    SunOS 5.8: /kernel/drv/hme and /kernel/drv/sparcv9/hme patch
108982    08        09    SunOS 5.8: fctl/fp/fcp/usoc driver patch
108983    08     CURRENT  SunOS 5.8: /kernel/drv/fcip driver patch
108984    07        08    SunOS 5.8: /kernel/drv/qlc driver patch
108985    03     CURRENT  SunOS 5.8: /usr/sbin/in.rshd patch
108987    09        12    SunOS 5.8: Patch for patchadd and patchrm
108989    02     CURRENT  SunOS 5.8: /usr/kernel/sys/acctctl and /usr/kernel/sys/exacctsys p
```

```
108991    18     CURRENT  Obsoleted by: 108827-15 SunOS 5.8: /usr/lib/libc.so.1 patch
108993    11        13    SunOS 5.8: nss and ldap patch
108995    01        04    SunOS 5.8: /usr/lib/libproc.so.1 patch
108997    03     CURRENT  SunOS 5.8: libexacct and libproject patch
108999    01     CURRENT  SunOS 5.8: PAM patch
109003    01     CURRENT  SunOS 5.8: /etc/init.d/acctadm and /usr/sbin/acctadm patch
109005    01        05    SunOS 5.8: /sbin/su.static and /usr/bin/su patch
109007    07        09    SunOS 5.8: at/atrm/batch/cron patch
109009    01        02    SunOS 5.8: /etc/magic and /usr/bin/file patch
109011    01     CURRENT  SunOS 5.8: /usr/bin/id and /usr/xpg4/bin/id patch
109013    02     CURRENT  SunOS 5.8: /usr/bin/lastcomm patch
109015    01     CURRENT  SunOS 5.8: /usr/bin/newtask patch
109017    01     CURRENT  SunOS 5.8: /usr/bin/pgrep and /usr/bin/pkill patch
109019    01        02    SunOS 5.8: /usr/bin/priocntl patch
109021    01     CURRENT  SunOS 5.8: /usr/bin/projects patch
109023    01     CURRENT  SunOS 5.8: /usr/bin/sparcv7/ps and /usr/bin/sparcv9/ps patch
109025    02        04    SunOS 5.8: /usr/bin/sparcv7/truss and /usr/bin/sparcv9/truss patch
109027    01     CURRENT  SunOS 5.8: /usr/bin/wracct patch
109029    01        02    SunOS 5.8: perl patch
109031    01     CURRENT  SunOS 5.8: projadd/projdel/projmod patch
109033    01     CURRENT  SunOS 5.8: /usr/bin/sparcv7/prstat and /usr/bin/sparcv9/prstat pat
109035    01        02    SunOS 5.8: useradd/userdel/usermod patch
109037    01     CURRENT  SunOS 5.8: /var/yp/Makefile and /var/yp/nicknames patch
109041    03        04    Obsoleted by: 108528-09 SunOS 5.8: sockfs patch
109043    02     CURRENT  SunOS 5.8: sonode adb macro patch
109045    02        03    SunOS 5.8: /usr/sbin/sparcv7/crash and /usr/sbin/sparcv9/crash pat
109077    01        11    SunOS 5.8: dhcp server and admin patch
109091    05     CURRENT  SunOS 5.8: /usr/lib/fs/ufs/ufsrestore patch
109128    01     CURRENT  SunOS 5.8: Provide conversion between codepages 1256 and ISO8859-6
109134    16        27    SunOS 5.8: WBEM patch
109137    01     CURRENT  Obsoleted by: 110934-03 SunOS 5.8: /usr/sadm/install/bin/pkginstal
109142    06     CURRENT  CDE 1.4: dtterm libDtTerm patch
109145    01     CURRENT  SunOS 5.8: /usr/sbin/in.routed patch
109147    16        21    SunOS 5.8: linker patch
109149    01        02    SunOS 5.8:: /usr/sbin/mkdevmaps and /usr/sbin/mkdevalloc patch
109152    01     CURRENT  SunOS 5.8: /usr/4lib/libc.so.1.9 and /usr/4lib/libc.so.2.9 patch
109154    05        16    WITHDRAWN PATCH SunOS 5.8: PGX32 Graphics
109159    01     CURRENT  SunOS 5.8: the mapping of zh_CN.euc%UTF-8 is consistent
109165    09        13    CDE 1.4: dtfile patch
109167    01     CURRENT  CDE 1.4: Desktop Help Updates Patch
109169    11        12    CDE 1.4: Window Manager Enhancements Patch
109181    04     CURRENT  Obsoleted by: 108528-13 SunOS 5.8: /kernel/fs/cachefs patch
109189    02        04    SunOS 5.8: ifp driver patch
109202    01        03    SunOS 5.8: /kernel/misc/gld and /kernel/misc/sparcv9/gld patch
109223    02     CURRENT  SunOS 5.8: kpasswd, libgss.so.1 and libkadm5clnt.so.1 patch
109234    02        09    SunOS 5.8: Apache Security and NCA Patch
109238    02     CURRENT  SunOS 5.8: /usr/bin/sparcv7/ipcs and /usr/bin/sparcv9/ipcs patch
109244    02
109277    02        03    SunOS 5.8: /usr/bin/iostat patch
109279    18     CURRENT  Obsoleted by: 108528-13 SunOS 5.8: /kernel/drv/ip patch
109318    27        28    SunOS 5.8: suninstall patch
109320    05        06    SunOS 5.8: LP Patch
109322    09     CURRENT  Obsoleted by: 108827-15 SunOS 5.8: libnsl patch
109324    04        05    SunOS 5.8: sh/jsh/rsh/pfsh patch
109326    08        09    SunOS 5.8: libresolv.so.2 and in.named patch
109328    01        03    SunOS 5.8: ypserv, ypxfr and ypxfrd patch
109354    06        17    CDE 1.4: dtsession patch
109384    01        06    SunOS 5.8: libaio patch
109454    01     CURRENT  SunOS 5.8: /kernel/fs/fifofs and /kernel/fs/sparcv9/fifofs patch
109458    01        03    SunOS 5.8: /kernel/strmod/ldterm patch
109460    03        09    SunOS 5.8: socal and sf drivers patch
109461    03     CURRENT  Obsoleted by: 111177-02 SunOS 5.8: /usr/lib/lwp/libthread.so.1 pat
109470    02     CURRENT  CDE 1.4: Actions Patch
109472    05        07    Obsoleted by: 108528-13 SunOS 5.8: /kernel/drv/tcp patch
109524    04        13    SunOS 5.8: /kernel/drv/ssd patch
109529    03        06     SunOS 5.8: luxadm, liba5k and libg_fc patch
109568    03     CURRENT  OpenWindows 3.6.2: sys-suspend need to support low power mode
109576    01     CURRENT  SunOS 5.8: mountall and fsckall patch
109582    01        02    CDE 1.4: sdtaudio patch
109587    03     CURRENT  Obsoleted by: 109318-18 SunOS 5.8: libspmistore patch
109607    01        02    SunOS 5.8: /usr/include/iso/stdlib_iso.h patch
109613    02        05    CDE 1.4: dtmail patch
109618    01     CURRENT  SunOS 5.8: en_US.UTF-8 locale patch
109639    02     CURRENT  Obsoleted by: 111188-02 SunOS 5.8: th locale has errors in / lacks
109642    01     CURRENT  SunOS 5.8: /usr/include/sys/dkio.h patch
109657    07        09    SunOS 5.8: isp driver patch
109667    04     CURRENT  SunOS 5.8: /usr/lib/inet/xntpd and /usr/sbin/ntpdate patch
109679    01     CURRENT  SunOS 5.8: /usr/share/lib/smartcard/ibutton.jar patch
109680    01     CURRENT  Obsoleted by: 108991-12 SunOS 5.8: nss_nisplus.so.1 and libnss_nis
109695    02        03    SunOS 5.8: /etc/smartcard/opencard.properties patch
109704    02     CURRENT  SunOS 5.8: Japanese iconv patch
```

```
109718    01
109727    01     CURRENT  SunOS 5.8: /usr/sadm/admin/printmgr/classes/pmclient.jar patch
109729    01     CURRENT  SunOS 5.8: /usr/bin/cat patch
109740    04     CURRENT  Obsoleted by: 108528-13 SunOS 5.8: /kernel/drv/udp patch
109742    04     CURRENT  Obsoleted by: 108528-13 SunOS 5.8: /kernel/drv/icmp patch
109748    01        03    CDE 1.4: sdtaudiocontrol patch
109754    03        05    SunOS 5.8: i2c driver patch
109764    02        04    SunOS 5.8: /kernel/fs/hsfs and /kernel/fs/sparcv9/hsfs patch
109766    02     CURRENT  SunOS 5.8: SUNWjxmft and SUNWjxcft patch for 8/10 dot font.
109783    01        02    SunOS 5.8: /usr/lib/nfs/nfsd and /usr/lib/nfs/lockd patch
109785    01     CURRENT  SunOS 5.8: /etc/inittab patch
109793    11        14    SunOS 5.8: su driver patch
109803    01     CURRENT  SunOS 5.8: /usr/bin/du and /usr/xpg4/bin/du patch
109805    10        15    SunOS 5.8: /usr/lib/security/pam_krb5.so.1 patch
109807    01     CURRENT  SunOS 5.8: /usr/sbin/dumpadm patch
109809    01     CURRENT  SunOS 5.8: timezone data patch for Australasia
109813    01     CURRENT  SunOS 5.8: /usr/include/memory.h patch
109815    04        15    SunOS 5.8: se, acebus, pcf8574, pcf8591 and scsb patch
109862    01        03    X11 6.4.1 Font Server patch
109872    01     CURRENT  SunOS 5.8: vis driver patch
109873    06        15    SunOS 5.8: prtdiag and platform libprtdiag_psr.so.1 patch
109874    06     CURRENT  Obsoleted by: 109896-07 SunOS 5.8: audio patch
109876    02     CURRENT  SunOS 5.8: fd driver patch
109877    01     CURRENT  SunOS 5.8: /usr/include/sys/dma_i8237A.h patch
109879    02     CURRENT  SunOS 5.8: isadma driver patch
109881    02     CURRENT  SunOS 5.8: 1394 adb macros patch
109882    06     CURRENT  SunOS 5.8: eri header files patch
109883    02     CURRENT  SunOS 5.8: /usr/include/sys/ecppsys.h patch
109885    09     CURRENT  SunOS 5.8: glm patch
109887    02        15    SunOS 5.8: smartcard and usr/sbin/ocfserv patch
109888    15        18    SunOS 5.8: platform drivers patch
109889    01        02    SunOS 5.8: usr platform links and libc_psr patch
109890    01     CURRENT  SunOS 5.8: pmserver.jar patch
109892    03     CURRENT  SunOS 5.8: /kernel/drv/ecpp driver patch
109893    02        04    SunOS 5.8: stc driver patch
109894    01     CURRENT  SunOS 5.8: /kernel/drv/sparcv9/bpp driver patch
109896    04        11    SunOS 5.8: USB and Audio Framework patch
109898    05     CURRENT  SunOS 5.8: /kernel/drv/arp patch
109900    01        02    SunOS 5.8: /etc/init.d/network and /sbin/ifparse patch
109902    03     CURRENT  SunOS 5.8: /usr/lib/inet/in.ndpd patch
109904    05     CURRENT  Obsoleted by: 108528-13 SunOS 5.8: /etc/default/mpathd and /sbin/i
109906    06     CURRENT  Obsoleted by: 108528-13 SunOS 5.8: dhcpagent, dhcpinfo, ifconfig a
109920    05        07    SunOS 5.8: pcic driver patch
109922    02        04    SunOS 5.8: pcelx and pcser driver patch
109924    02        04    SunOS 5.8: pcata driver patch
109926    02     CURRENT  SunOS 5.8: /kernel/drv/pem and /kernel/drv/sparcv9/pem patch
109928    04        05    SunOS 5.8: pcmem and pcmcia patch
109931    01        05    CDE 1.4: sdtimage Patch
109933    01     CURRENT  SunOS 5.8: mv, cp, ln patch
109935    02        03    SunOS 5.8: libprtdiag_psr.so.1 for SUNW,UltraSPARC-IIi-Netract pat
109936    01     CURRENT  SunOS 5.8: /usr/bin/diff patch
109953    02
109954    01     CURRENT  Obsoleted by: 108528-13 SunOS 5.8: /kernel/sys/pset and /kernel/sy
109960    01     CURRENT  CDE 1.4: sdtperfmeter patch
109965    02        03    Obsoleted by: 109887-02 SunOS 5.8: pam_smartcard.so.1 patch
109990    01     CURRENT  SunOS 5.8: /usr/ccs/bin/dis patch
109994    01     CURRENT  SunOS 5.8: /usr/bin/sparcv7/adb and /usr/bin/sparcv9/adb patch
110068    01        02    CDE 1.4: PDASync patch
110075    01     CURRENT  SunOS 5.8: /kernel/drv/devinfo and /kernel/drv/sparcv9/devinfo pat
110088    02     CURRENT  CDE 1.4: DtPower patch
110127    02        04    SunOS 5.8: Generic Framebuffer configuration GraphicsPatch
110165    01        04    SunOS 5.8: /usr/bin/sed patch
110221    03        06    SunOS 5.8:  Dcam1394 patch
110269    01     CURRENT  SunOS 5.8: /usr/lib/libnisdb.so.2 patch
110274    03     CURRENT  SunOS 5.8: Figgs Custom install new features and install help
110283    05        06    SunOS 5.8: mkfs and newfs patch
110285    01     CURRENT  SunOS 5.8: consconfig_dacf patch
110286    08        10    OpenWindows 3.6.2: Tooltalk patch
110320    01     CURRENT  SunOS 5.8: /kernel/misc/sparcv9/s1394 patch
110322    01        02    SunOS 5.8: /usr/lib/netsvc/yp/ypbind patch
110326    02     CURRENT  CDE 1.4: dtstyle patch
110335    02     CURRENT  CDE 1.4: dtprintinfo patch
110368    01        02    SunOS 5.8: pcf8574 driver patch for SUNW Sun-Fire-280R
110369    04        05    SunOS 5.8: sgcn patch
110370    02        03    SunOS 5.8: SUNW,Sun-Fire usr platform links patch
110371    02        03    SunOS 5.8: serengeti support, Update3, sgfru patch
110373    02        04    SunOS 5.8: /platform/SUNW,Sun-Fire/kernel/drv/sparcv9/sgsbbc patch
110374    06        08    SunOS 5.8: /platform/SUNW,Sun-Fire/kernel/drv/sparcv9/sgenv patch
110375    02        05    SunOS 5.8: /platform/SUNW,Sun-Fire/kernel/drv/sparcv9/ssm patch
110376    01     CURRENT  SunOS 5.8: littleneck support, usr_platform patch, S8 Update 3
110378    05        06    SunOS 5.8: mipagent patch Mobile IP
```

```
110379    01     CURRENT  SunOS 5.8: littleneck support, gpio patch
110380    04     CURRENT  SunOS 5.8: ufssnapshots support, libadm patch
110381    01     CURRENT  SunOS 5.8: ufssnapshots support, clri patch
110382    01        02    SunOS 5.8: ufssnapshots support, fssnap kernel, S8 Update 3
110383    02     CURRENT  Obsoleted by: 108528-13 SunOS 5.8: libnvpair patch
110384    05     CURRENT  Obsoleted by: 108528-11 SunOS 5.8: RCM libraries & header patch
110385    03     CURRENT  SunOS 5.8: RCM modules patch
110386    01        02    SunOS 5.8: RBAC Feature Patch
110387    03     CURRENT  SunOS 5.8: ufssnapshots support, ufsdump patch
110388    01     CURRENT  SunOS 5.8: RBAC Feature for Solaris Update 3
110389    02        05    SunOS 5.8: cvc CPU signature
110390    01        02    Obsoleted by: 108993-05 SunOS 5.8: ldapclient patch
110407    02     CURRENT  CDE 1.4 Sdttypes patch
110423    01
110453    03     CURRENT  SunOS 5.8: admintool patch
110457    01        05    SunOS 5.8: scmi2c driver patch
110458    02     CURRENT  SunOS 5.8: libcurses patch
110460    20        26    SunOS 5.8: fruid/PICL plug-ins patch
110461    01     CURRENT  SunOS 5.8: ttcompat patch
110499    03     CURRENT  Obsoleted by: 108652-29 X11 6.4.1: Xsun patch
110511    01        05    SunOS 5.8: rpc.nisd patch
110597    02
110600    02
110603    01     CURRENT  CDE 1.4: sdtname patch
110609    01        03    SunOS 5.8: cdio.h and command.h USB header patch
110611    01     CURRENT  SunOS 5.8: lp.cat and postio ECP patch
110615    05     CURRENT  SunOS 5.8: sendmail patch
110662    07        10    SunOS 5.8: ksh patch
110668    03     CURRENT  SunOS 5.8: /usr/sbin/in.telnetd patch
110670    01     CURRENT  SunOS 5.8: usr/sbin/static/rcp patch
110700    01     CURRENT  SunOS 5.8: automount patch
110712    03
110716    02     CURRENT  SunOS 5.8: Solaris Product Registry 3.0 patch
110723    05     CURRENT  SunOS 5.8: /kernel/drv/sparcv9/eri patch
110724    01     CURRENT  SunOS 5.8: liblayout patch
110750    01     CURRENT  SunOS 5.8: TCX Graphics Patch
110791    01
110794    01        05    SunOS 5.8: dr_daemon patch
110797    02     CURRENT  SunOS 5.8: UR4 New int
110811    01     CURRENT  SunOS 5.8: libnls patch
110813    01     CURRENT  SunOS 5.8: libxfn patch
110815    01     CURRENT  SunOS 5.8:  libmp patch
110817    01     CURRENT  SunOS 5.8: apptrace and interceptors patch
110819    01        03    SunOS 5.8: /platform/sun4u/kernel/drv/sparcv9/us patch
110820    02        10    SunOS 5.8: /platform/SUNW,Sun-Fire-15000/kernel/drv/sparcv9/dman p
110821    01        02    SunOS 5.8: iosram driver patch
110822    01     CURRENT  SunOS 5.8: mboxsc driver patch
110823    03        04    SunOS 5.8: fcode patch
110824    02        03    SunOS 5.8: fcpci driver patch
110825    02        03    SunOS 5.8: fcodem driver patch
110826    02        06    SunOS 5.8: SUNW,Sun-Fire-15000/kernel/drv/sparcv9/schpc patch
110827    01        02    SunOS 5.8: scosmb driver patch
110828    01        02    SunOS 5.8: sbbc driver patch
110829    01        02    SunOS 5.8: /platform/sun4u/kernel/tod/sparcv9/todstarcat patch
110830    01        02    SunOS 5.8: /platform/SUNW,Sun-Fire-15000/lib/cvcd patch
110831    02     CURRENT  SunOS 5.8: /platform/SUNW,Sun-Fire-15000/kernel/drv/sparcv9/cvc pa
110832    01     CURRENT  SunOS 5.8: cvcredir patch
110833    01     CURRENT  SunOS 5.8: usr platform links
110834    02        03    Obsoleted by: 109873-11 SunOS 5.8: SUNW,Sun-Fire-15000 libprtdiag_
110835    02        05    SunOS 5.8: platform/sun4u/kernel/misc/sparcv9/gptwo_cpu patch
110836    02        04    SunOS 5.8: /platform/sun4u/kernel/misc/sparcv9/gptwocfg patch
110837    03     CURRENT  SunOS 5.8: efcode patch
110838    05        06    SunOS 5.8: /platform/SUNW,Sun-Fire-15000/kernel/drv/sparcv9/axq pa
110839    01        03    SunOS 5.8: /usr/lib/rcm/modules/SUNW_ip_rcm.so patch
110840    01        03    SunOS 5.8: bbc patch
110841    01     CURRENT  SunOS 5.8: gptwo patch
110842    01        09    SunOS 5.8: hpc3130 driver patch for SUNW,Sun-Fire-880
110843    01        03    Obsoleted by: 110849-06 SunOS 5.8: libprtdiag_psr.so.1 patch for S
110844    01        02    SunOS 5.8: /platform/sun4u/kernel/drv/sparcv9/lm75 patch
110845    01        03    SunOS 5.8: /platform/sun4u/kernel/drv/sparcv9/ltc1427patch
110846    01        02    SunOS 5.8: /platform/sun4u/kernel/drv/sparcv9/pcf8574patch
110847    01        02    SunOS 5.8: /platform/sun4u/kernel/drv/sparcv9/pcf8591patch
110848    02     CURRENT  SunOS 5.8: pcicfg patch
110849    01        12    SunOS 5.8: PICL support for SUNW,Sun-Fire-880
110850    01     CURRENT  Obsoleted by: 108528-11 SunOS 5.8: sbdp patch
110851    01        02    SunOS 5.8: /platform/sun4u/kernel/drv/sparcv9/ssc050 patch
110852    01        03    SunOS 5.8: /platform/sun4u/kernel/drv/sparcv9/ssc100 patch
110853    01     CURRENT  SunOS 5.8: SUNW,Sun-Fire-880 usr platform links patch
110854    01        02    SunOS 5.8: /platform/sun4u/kernel/drv/sparcv9/smbus_ara patch
110856    01     CURRENT  SunOS 5.8: /etc/inet/services patch
110888    01     CURRENT  SunOS 5.8 : figgs, New and updated message strings
```

```
110896    01        02    SunOS 5.8: cachefs/mount patch
110898    04        08    SunOS 5.8: csh/pfcsh patch
110900    01        07    SunOS 5.8: /platform/sun4u/kernel/misc/sparcv9/pcicfg.e patch
110901    01     CURRENT  SunOS 5.8: /kernel/drv/sgen and /kernel/drv/sparcv9/sgen patch
110903    05     CURRENT  SunOS 5.8: edit, ex, vedit, vi and view patch
110905    01        02    SunOS 5.8: /usr/bin/find patch
110907    01     CURRENT  SunOS 5.8: /usr/include/arpa/inet.h patch
110910    01     CURRENT  SunOS 5.8: /usr/lib/fs/ufs/fsck patch
110912    01        03    SunOS 5.8: cfgadm patch
110914    01     CURRENT  SunOS 5.8: /usr/bin/tr patch
110916    03     CURRENT  SunOS 5.8: sort patch
110918    01        04    SunOS 5.8: /kernel/drv/openeepr and prtconf patch
110927    01     CURRENT  SunOS 5.8: Need to backport fixes in SUNW_PKGLIST in s8u4
110934    08        10    SunOS 5.8: pkgtrans, pkgadd, pkgchk and libpkg.a patch
110939    01     CURRENT  SunOS 5.8: /usr/lib/acct/closewtmp patch
110943    01     CURRENT  SunOS 5.8: /usr/bin/tcsh patch
110945    06        07    SunOS 5.8: /usr/sbin/syslogd patch
110951    02        03    SunOS 5.8: /usr/sbin/tar and /usr/sbin/static/tar patch
110957    02     CURRENT  SunOS 5.8: /usr/bin/mailx patch
111069    01     CURRENT  SunOS 5.8: bsmunconv overwrites root cron tab if cu created /tmp/r
111071    01     CURRENT  SunOS 5.8: cu patch
111073    01     CURRENT  SunOS 5.8: re_comp header patch
111085    02     CURRENT  SunOS 5.8: /usr/bin/login patch
111088    01        02    SunOS 5.8: mdb patch
111098    01     CURRENT  SunOS 5.8: ROC timezone should be avoided for political reasons
111111    03     CURRENT  SunOS 5.8: /usr/bin/nawk patch
111177    06     CURRENT  Obsoleted by: 108827-15 SunOS 5.8: /usr/lib/lwp/libthread.so.1 pat
111232    01     CURRENT  SunOS 5.8: patch in.fingerd
111234    01     CURRENT  SunOS 5.8: patch finger
111293    04     CURRENT  SunOS 5.8: /usr/lib/libdevinfo.so.1 patch
111310    01     CURRENT  SunOS 5.8: /usr/lib/libdhcpagent.so.1 patch
111325    02     CURRENT  SunOS 5.8: /usr/lib/saf/ttymon patch
111327    05     CURRENT  SunOS 5.8: libsocket patch
111504    01     CURRENT  SunOS 5.8: /usr/bin/tip patch
111548    01     CURRENT  SunOS 5.8: catman, man, whatis, apropos and makewhatis patch
111570    01        02    SunOS 5.8: uucp patch
111596    02     CURRENT  SunOS 5.8: /usr/lib/netsvc/yp/rpc.yppasswdd patch
111606    02     CURRENT  SunOS 5.8: /usr/sbin/in.ftpd patch
111626    01        03    OpenWindows 3.6.2: Xview Patch
111659    07     CURRENT  SunOS 5.8: passwd and pam_unix.so.1 patch
111826    01     CURRENT  SunOS 5.8: /usr/sbin/sparcv7/whodo & /usr/sbin/sparcv9/whodo patch
111874    05        06    SunOS 5.8: usr/bin/mail patch
111881    02        03    SunOS 5.8: /usr/kernel/strmod/telmod patch
111958    02     CURRENT  SunOS 5.8: /usr/lib/nfs/statd patch
112138    01     CURRENT  SunOS 5.8:: usr/bin/domainname patch
112218    01     CURRENT  SunOS 5.8:: pam_ldap.so.1 patch
112237    05        07    SunOS 5.8: mech_krb5.so.1 patch
112254    01     CURRENT  SunOS 5.8: /kernel/sched/TS patch
112325    01     CURRENT  SunOS 5.8: /kernel/fs/udfs and /kernel/fs/sparcv9/udfs patch
112396    02     CURRENT  SunOS 5.8: /usr/bin/fgrep patch
112425    01     CURRENT  SunOS 5.8: /usr/lib/fs/ufs/mount and /etc/fs/ufs/mount patch
112459    01     CURRENT  SunOS 5.8: /usr/lib/pt_chmod patch
112611    01     CURRENT  SunOS 5.8: /usr/lib/libz.so.1 patch
112668    01     CURRENT  SunOS 5.8: /usr/bin/gzip patch
112796    01     CURRENT  SunOS 5.8: /usr/sbin/in.talkd patch
112846    01     CURRENT  SunOS 5.8: /usr/lib/netsvc/rwall/rpc.rwalld patch
================================================================================

UNINSTALLED RECOMMENDED PATCHES

Patch  Ins Lat Age  Require    Incomp  Synopsis
  ID   Rev Rev       ID         ID
------ --- --- --- ---------- --------- ----------------------------------------
109221 N/A  06 745 108993-01           Obsoleted by: 109318-12 SunOS 5.8: Patch
for sysidnet
109951 N/A  01 907                     SunOS 5.8: jserver buffer overflow
110949 N/A  01 572                     Obsoleted by: 110934-04 SunOS 5.8: /usr/s
adm/install/bin/pkgremove
111090 N/A  03 553                     Obsoleted by: 108993-05 SunOS 5.8: /usr/l
ib/libsldap.so.1 patch
111299 N/A  04 157 110386-01           SunOS 5.8: PPP patch
111321 N/A  03 131                     SunOS 5.8: klmmod and klmops patch
111363 N/A  01 635                     Obsoleted by: 110934-04 SunOS 5.8: /usr/s
bin/installf patch
111879 N/A  01 532                     SunOS 5.8: Solaris Product Registry patch
 SUNWwsr
111883 N/A  14  83                     SunOS 5.8: Sun GigaSwift Ethernet 1.0 dri
ver patch
112279 N/A  02 255                     SunOS 5.8: pkgrm failed during upgrade fr
om Solaris 8 to Solaris 9
112334 N/A  02 342                     Obsoleted by: 108528-14 SunOS 5.8: /usr/i
```

```
nclude/sys/archsystm.h pa
113650 N/A  01  33                    SunOS 5.8: /usr/lib/utmp_update patch
113792 N/A  01  77                    OpenWindows 3.6.2: mailtool patch
================================================================================

UNINSTALLED SECURITY PATCHES

NOTE: This list includes the Security patches that are also Recommended

Patch  Ins Lat Age  Require    Incomp  Synopsis
  ID   Rev Rev        ID         ID
------ --- --- --- --------- --------- ----------------------------------------
108979 N/A  10 817 108528-03           Obsoleted by: 108528-04 SunOS 5.8: platfo
rm nexus, I2C, Netra ct a
109951 N/A  01 907                    SunOS 5.8: jserver buffer overflow
110416 N/A  03 557                    SunOS 5.8: ATOK12 patch
110953 N/A  04  48 108528-18          SunOS 5.8: /usr/kernel/drv/llc2 patch
110955 N/A  04  48 108528-18          SunOS 5.8: /kernel/strmod/timod patch
111090 N/A  03 553                    Obsoleted by: 108993-05 SunOS 5.8: /usr/l
ib/libsldap.so.1 patch
111299 N/A  04 157 110386-01          SunOS 5.8: PPP patch
111321 N/A  03 131                    SunOS 5.8: klmmod and klmops patch
111332 N/A  06  35                    SunOS 5.8: /usr/lib/dcs patch
111400 N/A  01 600                    SunOS 5.8: KCMS configure tool has a secu
rity vulnerability
111588 N/A  04  48 108528-18          SunOS 5.8: /kernel/drv/ws and /kernel/fs/
specfs patch
111624 N/A  04 131                    SunOS 5.8: /usr/sbin/inetd patch
111647 N/A  01 553                    BCP libmle buffer overflow
112039 N/A  01 511                    SunOS 5.8: usr/bin/ckitem patch
112390 N/A  07  26 109223-02          SunOS   5.8:   Supplemental   Encryption   Kerberos   V5:
mech_krb5.so.1
112438 N/A  01 319                    SunOS 5.8: /kernel/drv/random patch
112605 N/A  04 157 108993-11         SunOS 5.8: /kernel/fs/autofs and /usr/lib/autofs/automountd
patch 111023-02
112792 N/A  01 216 108968-06          SunOS 5.8: /usr/lib/pcmciad patch
113650 N/A  01  33                    SunOS 5.8: /usr/lib/utmp_update patch
113652 N/A  03  49 108528-17 108528-18 (or newer) SunOS 5.8: Supplemental Kernel
 Update Patch for 108528-17
113685 N/A  02  11 108528-18          SunOS 5.8: logindmux/ptsl/ms/bufmod/llc1/
kb/zs/zsh/ptem patch
113687 N/A  01  48 108528-18          SunOS 5.8: /kernel/misc/kbtrans patch
113792 N/A  01  77                    OpenWindows 3.6.2: mailtool patch
114146 N/A  01  63 108528-16 108528-17 (or newer) SunOS 5.8: Supplemental Kernel
 Update Patch for 108528-16
================================================================================

UNINSTALLED Y2K PATCHES

NOTE: This list includes the Y2K patches that are also Recommended

Patch  Ins Lat Age  Require    Incomp  Synopsis
  ID   Rev Rev        ID         ID
------ --- --- --- --------- --------- ----------------------------------------
All Y2K patches installed!
```

Endnotes

1 "GIAC Information Security Practices and Procedures." GIAC internal document 19 Jul. 2002.

2 "GIAC Disaster Recovery Procedures." GIAC internal document 18 Apr. 2002.

3 "ICAT Metabase Documentation." URL: http://icat.nist.gov/icat_documentation.htm (5 Feb. 2003).

4 "Free Sun Alert Notifications Article 48879." 20 Dec. 2002. URL: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/48879 (27 Jan. 2003).

5 "CERT Advisory CA-2002-34 Buffer Overflow in Solaris X Windows Font Service." 17 Dec. 2002. URL: http://www.cert.org/advisories/CA-2002-34.html (25 Jan. 2003).

6 "Vulnerability Note VU#683673." 6 Dec. 2002. URL: http://www.kb.cert.org/vuls/id/683673 (27 Jan. 2003).

7 "CAN-2002-1296." 23 Dec. 2002. URL: http://icat.nist.gov/icat.cfm?cvename=CAN-2002-1296 (27 Jan.2002).

8 "Free Sun Alert Notifications Article 46022." 31 Jan. 2003. URL: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/46022 (2 Feb. 2003).

9 "Free Sun Alert notifications Article 50104." 23 Jan. 2003. URL: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/50104 (27 Jan. 2003).

10 "Free Sun Alert Notifications Article 46122." 23 Dec. 2002. URL: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/46122 (27 Jan. 2003).

11 "Vulnerability Note VU#192995." 3 Oct. 2002. URL: http://www.kb.cert.org/vuls/id/192995 (27 Jan. 2003).

12 "Free Sun Alert Notifications Article 47815." 2 Jan. 2003. URL: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/47815 (27 Jan. 2003).

13 "CERT Advisory CA-2002-17 Apache Web Server Chunk Handling Vulnerability." 25 Sept 2002. URL: http://www.cert.org/advisories/CA-2002-17.html (27 Jan. 2003).

[14] "CERT/CC Vulnerability Note VU#698467." 27 Feb. 2002.
URL: http://www.kb.cert.org/vuls/id/698467 (27 Jan. 2003).

[15] "CERT/CC Vulnerability Note VU#168795." 26 Feb. 2002.
URL: http://www.kb.cert.org/vuls/id/168795 (27 Jan. 2003).

[16] "GIS Advisory ID: 2002041701." 25 Apr. 2002.
URL: http://www.globalintersec.com/adv/sudo-2002041701.txt (28 Jan. 2003).

[17] "Sudo Prompt Buffer Overflow."
URL: http://www.courtesan.com/sudo/alerts/prompt.html (28 Jan. 2003).

[18] "Oracle Security Alert #45." 4 Oct. 2002.
URL: http://technet.oracle.com/deploy/security/pdf/2002alert45rev4.pdf
(28 Jan. 2003).

[19] Conoboy, Brendan, Fichtner, Erik. "IP Filter Based Firewall HOWTO."
11 Dec. 2002.URL: http://www.obfuscation.org/ipf/ipf-howto.txt (29 Jan. 2003).

[20] "Solaris Benchmark v1.1.0." Oct 22, 2002.
URL: http://www.cisecurity.org/bench_solaris.html (30 Jan. 2003).

[21] "coreadm(1M)." 11 Nov. 1999.
URL: http://docs.sun.com/db/doc/806-0625/6j9vfilko?q=%22coreadm%22&a=view
(29 Jan. 2003).

[22] "CERT/CC Vulnerability Note VU#698467." 26 Feb. 2002
URL: http://www.kb.cert.org/vuls/id/698467 (28 Jan. 2003).

[23] Litchfield, David. "Hackproofing Oracle Application Server." 5 Feb. 2002.
URL: http://www.nextgenss.com/papers/hpoas.pdf (27 Jan. 2003).