



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at <http://www.giac.org/registration/gsec>

Know your Weak Points early enough - Alert Services: What is the benefit of a Commercial Service (Symantec DeepSight Alert Services)?

Stefan Mueller, April 9, 2003

1. Overview

Today it is very important to receive information about vulnerabilities, cyber attacks and malicious code as soon as possible. Enterprises are threatened by attacks continuously. Through the use of vulnerabilities, hackers often can attack and penetrate corporate networks successfully.

Using many different technologies, it is very complicated and time-consuming to keep these systems in a current, secure state.

Only a few years ago, often no information about vulnerabilities was available from the vendors of appliances, operating systems or applications. Today vendors inform their customers on websites or via mailing lists. Information about software patches is available as soon as possible.

Receiving this information quickly is extremely important for companies. Only secure systems offer protection against attacks.

The Symantec Internet Security Threat Report, for example, provides the Internet community with a deeper understanding of how Internet threats are evolving over time. For the year 2002 the following trends can be seen:

- blended threats continue to present the greatest risk to the Internet community
- excluding worm and blended threat activity, measured cyber attack volume declined slightly
- the discovery rate for new IT product vulnerabilities accelerated substantially

The majority of documented vulnerabilities were easily exploitable either because sophisticated tools were widely available or because exploit tools were not required at all. Within hours of release many of these threats spread rapidly among Internet-connected organizations.

Keeping systems up-to-date is the new challenge of today's business.

2. Resources and Alerting Services

A Company has to monitor multiple mailings lists and websites to collect all information about

- Network Appliances

- Operating Systems
- Server Applications
- Desktop Applications
- etc.

used in their environment. Visiting web sites from vendors like Microsoft, Cisco or Oracle is a daily task to get information about possible vulnerabilities. The websites from security vendors like Symantec or McAfee have to be visited to get information about malicious code or cyber attacks. Furthermore the websites from independent organizations like SANS or CERT delivers information and best practices for security reasons.

But the question always is - which information is relevant to the company's environment?

A commercial service like Symantec DeepSight Alert Services provides personalized vulnerability and malicious code alerts. The service delivers detailed notification of potential threats as they're identified, providing actionable information to help users mitigate threats before they can be exploited.

3. Free Alerting Services and Resources

3.1 - Microsoft Security Bulletin (subscription service)

With Microsoft Security Bulletin Microsoft delivers a free E-mail notification service to send information to subscribers about the security of Microsoft products.

Microsoft Security Bulletins provide accurate information to customers that they can use to learn about and help protect their systems against attacks. The Microsoft security team inspect issues reported to Microsoft, as well as issues discussed in security newsgroups. When Microsoft publish bulletins, they will contain information

- on what the issue is
- what products it affects
- how customers can take steps to protect their systems against it
- links to other sources of information

on the issue.

Subscribers receive an E-mail message each time an update is released. The Update explains why Microsoft issues the update, lists which products are affected, and provides a link to the full announcement on the Security and Privacy Web site.

This is a sample of a Security Bulletin concerning a Microsoft 2000 operating system vulnerability:

-----BEGIN PGP SIGNED MESSAGE-----

- - - - -
Title: Unchecked buffer in Windows component could cause web
server compromise (815021)
Date: 17 March, 2003
Software: Microsoft Windows 2000
Impact: Run Code of Attacker's Choice
Max Risk: Critical
Bulletin: MS03-007

Microsoft encourages customers to review the Security Bulletins
at:
<http://www.microsoft.com/technet/security/bulletin/MS03-007.asp>
http://www.microsoft.com/security/security_bulletins/ms03-007.asp
- - - - -

Issue:
=====

Microsoft Windows 2000 supports the World Wide Web Distributed
Authoring and Versioning (WebDAV) protocol. WebDAV, defined in
RFC 2518, is a set of extensions to the Hyper Text Transfer
Protocol (HTTP) that provide a standard for editing and file
management between computers on the Internet. A security
vulnerability is present in a Windows component used by WebDAV,
and results because the component contains an unchecked buffer.

An attacker could exploit the vulnerability by sending a
specially formed HTTP request to a machine running Internet
Information Server (IIS). The request could cause the server to
fail or to execute code of the attacker's choice. The code would
run in the security context of the IIS service (which, by
default, runs in the LocalSystem context).

Although Microsoft has supplied a patch for this vulnerability
and recommends customers install the patch immediately,
additional tools and preventive measures have been provided that
customers can use to block the exploitation of this vulnerability
while they are assessing the impact and compatibility of the
patch. These temporary workarounds and tools are discussed in the
"Workarounds" section in the FAQ below.

Mitigating Factors:

=====

- URLScan, which is a part of the IIS Lockdown Tool will block
this attack in its default configurations
- The vulnerability can only be exploited remotely if an
attacker can establish a web session with an affected server

Risk Rating:

=====

- Critical

Patch Availability:

=====

- A patch is available to fix this vulnerability. Please read
the Security Bulletins at

<http://www.microsoft.com/technet/security/bulletin/ms03-007.asp>
http://www.microsoft.com/security/security_bulletins/ms03-007.asp

for information on obtaining this patch.

THE INFORMATION PROVIDED IN THE MICROSOFT KNOWLEDGE BASE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. MICROSOFT DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL MICROSOFT CORPORATION OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF MICROSOFT CORPORATION OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES SO THE FOREGOING LIMITATION MAY NOT APPLY.

-----BEGIN PGP SIGNATURE-----
Version: PGP 7.1

iQEVAwUBPnYUXY0ZSRQxA/UrAQG43Af/d+IndquMNQlQLS2LjEFwBy5bh+np051f
fu65SMf6L5owLobpzMvprwKtqSVdLLco3ynyi76Vq4VG52suh1ft+B7AbVNaKEkG
///qWiBQThiTTIw5qwgW+x7h/O6bvIKUvK1O/LdU8WGpph7ZCInA2dSXxo4hwJyM
J4UJeKntGc4VqcTzzI1lq+ebgy5q3XEjDep89H49D836h0hRJyWzzzD4pgm/YtFg
JpARG9nkrUEj50cVKEPTggBaHVMxV7agJL7XrmytelXa4yUUia8r7R0SdpNTJc0X
FO5daVtgx6hIY22ryRlPumqQ7K40Z5iBhfd1hHNpPvasucj++/ytKQ==
=e404

-----END PGP SIGNATURE-----

You have received this e-mail bulletin because of your subscription to the Microsoft Product Security Notification Service. For more information on this service, please visit <http://www.microsoft.com/technet/security/notify.asp>.

To verify the digital signature on this bulletin, please download our PGP key at <http://www.microsoft.com/technet/security/notify.asp>.

To unsubscribe from the Microsoft Security Notification Service, please visit the Microsoft Profile Center at <http://register.microsoft.com/regsys/pic.asp>

If you do not wish to use Microsoft Passport, you can unsubscribe from the Microsoft Security Notification Service via email as described below:
Reply to this message with the word UNSUBSCRIBE in the Subject line.

For security-related information about Microsoft products, please visit the Microsoft Security Advisor web site at <http://www.microsoft.com/security>.

Sample 1 - http://www.microsoft.com/security/security_bulletins/ms03-007.asp

3.2 - SANS Critical Vulnerability Analysis (subscription service)

The Critical Vulnerability Analysis report from SANS is delivered once a week. It focuses on the most important vulnerabilities and tells what damage they do.

This is a section of a SANS Critical Vulnerability Analysis report about important vulnerabilities and attacks identified during a week:

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

```
*****
SANS Critical Vulnerability Analysis
March 24, 2003                               Vol. 2. No. 11
*****
```

The weekly CVA prioritizes and summarizes the most important vulnerabilities and attacks identified during the past week and provides guidance on appropriate actions to protect your systems.

```
*****
```

Table of Contents:

Widely Deployed Software

- (1) CRITICAL: SUN XDR Library XDRMEM_GETBYTES Integer Overflow
- (2) CRITICAL: Microsoft Windows 2000 ntdll.dll Buffer Overflow
- (3) CRITICAL: Kerberos v4 Multiple Protocol Weaknesses
- (4) HIGH: Samba SMB/CIFS Packet Reassembly Buffer Overflow
- (5) MODERATE: Microsoft Windows Script Engine Integer Overflow
- (6) MODERATE: BEA WebLogic Unprotected Internal Applications
- (7) MODERATE: OpenSSL Timing Attack Private Key Disclosure

Other Software

- (8) MODERATE: McAfee ePolicy Orchestrator Format String Vulnerability

```
***** Sponsored Links *****
Privacy notice: These links redirect to non-SANS web pages.
```

GFI LANguard S.E.L.M.: Event-log-based intrusion detection and network-wide event log management - Download free starter-pack!

<http://www.sans.org/cgi-bin/sanspromo/CVA29>

Stop spam! Learn the Top 10 enterprise techniques to control spam
***request the white paper

<http://www.sans.org/cgi-bin/sanspromo/CVA30>

Instantly stop DDoS attacks and port scans. Hands-on, online demo-launch and mitigate live attacks.

<http://www.sans.org/cgi-bin/sanspromo/CVA31>

```
*****
```

Widely Deployed Software

- ```

```
- (1) CRITICAL: SUN XDR Library XDRMEM\_GETBYTES Integer Overflow

#### Affected Products:

Applications using vulnerable implementations of SunRPC-derived XDR libraries, including:

- \* SUN Microsystems network services library (libnsl)
- \* BSD-derived libraries with XDR/RPC routines (libc)
- \* GNU C library with SunRPC (glibc)

#### Description:

The SUN Microsystems XDR libraries provide a platform-independent mechanism for applications to converse over the network. These libraries are widely used in RPC implementations that run on multiple platforms. An integer overflow vulnerability exists the XDRMEM\_GETBYTES library function, making any application linked against an affected library potentially vulnerable. An example showing how to trigger

the bug via a malformed call to the Solaris rpcbind service has been posted. Because RPC services often run as root, exploitation of this flaw can result in remote root compromise. This vulnerability was previously reported in the February 17, 2003 CVA (item #2).

Risk: Remote compromise.

Remotely exploitable buffer overflows in multiple applications, which can lead to the execution of arbitrary code with root privileges. There have also been reports of being able to crash the rpcbind service.

Deployment: Widely deployed. Affected products/vendors include: Cray, FreeBSD, Linux (Caldera, Conectiva, Debian, EnGarde, Mandrake, Openwall, RedHat, SuSE, Trustix), HP-UX, AIX, Kerberos 5, OpenAFS, OpenBSD, IRIX and Solaris.

Ease of Exploitation: Unknown.

A few examples of how to exploit the condition to cause a DoS are available, no exploits enabling system compromise have yet been released.

Status: Some vendors have confirmed and are providing patches; others are still investigating the problem. Consult the CERT advisory and SecurityFocus pages to find a patch from your vendor.

#### References:

CERT Advisory and Vulnerability Note  
<http://www.cert.org/advisories/CA-2003-10.html>  
<http://www.kb.cert.org/vuls/id/516825>

#### eEye Advisory

<http://www.eeye.com/html/Research/Advisories/AD20030318.html>

Previous report in 2/17/03 SANS CVA (item #2):

[http://www.sans.org/newsletters/cva/vol2\\_6.php](http://www.sans.org/newsletters/cva/vol2_6.php)

Early Leak of Advisory to Full Disclosure List (3/16/03)

<http://lists.netsys.com/pipermail/full-disclosure/2003-March/004526.html>

News Article about Leaks

<http://www.ds-osac.org/view.cfm?key=7E4457414B50&type=2B170C1E0A3A0F162820>

SecurityFocus BID

<http://www.securityfocus.com/bid/7123>

#### Council Site Actions:

Most of the reporting council sites are still evaluating the criticality of this vulnerability (due to the conflicting reports) and have notified their Unix support departments. Almost all sites plan to roll out the patches when they become available. Most of the sites reported that they block incoming RPC-based services at their network perimeters, which helps mitigate or reduce the threat of this problem.

\*\*\*\*\*

**Sample 2 - The complete sample of the Critical Vulnerability Analysis report is published at [http://www.sans.org/newsletters/cva/vol2\\_11.php](http://www.sans.org/newsletters/cva/vol2_11.php) on the newsletters and digests section at the SANS web site.**

### 3.3 - AVERT Virus News (subscription service)

McAfee AVERT (Anti-Virus Emergency Response Team) is a division of McAfee. The responsibility is to support the internet public and McAfee's customers. They help users work more securely by exploring threats.

Three integrated teams work together to provide Services and Support, Analysis, and Advanced Research on Viruses.

AVERT works together with McAfee's customers and the research community on the internet to provide virus security services, information, diagnostics and protection from new viruses.

This is a sample of a E-mail notification from AVERT Virus News concerning the Code Red.F-worm:

#### Notice

This is a Low-Profiled Virus Notice for W32/CodeRed.f.worm. AVERT does not consider this a higher risk than Low-Profiled due to detection of this existing in dat files available since August 6th, 2001, and due to customers having already taken the precaution of updating their systems in response to the initial CodeRed worm.

#### Justification

This W32/CodeRed.f.worm has been deemed Low-Profiled due to Media Attention at <http://www.theregister.co.uk/content/56/29724.html>. W32/CodeRed.f.worm is referred to as CodeRed-F within the article.

#### Read About It

Information about W32/CodeRed.f.worm is located on VIL at:  
[http://vil.nai.com/vil/content/v\\_100142.htm](http://vil.nai.com/vil/content/v_100142.htm).

#### Detection

W32/CodeRed.f.worm was first discovered on March 11th, 2003 and detection has been available since the 4152 dat files, as W32/CodeRed.gen.worm (Release Date: August 6th, 2001).

To stay updated and protected download the latest dat files from  
<http://www.mcafeeb2b.com/naicommon/download/dats/find.asp>.

#### Risk Assessment Definition

For further information on the Risk Assessment and AVERT Recommended Actions please see:  
<http://www.mcafeeb2b.com/naicommon/avert/virus-alerts/avert-risk-assessment.asp>

Regards

AVERT

---

You are currently subscribed to avertalert as: [smueller@symantec.com](mailto:smueller@symantec.com)  
To unsubscribe send a blank email to [leave-avertalert-131596T@listserv.nai.com](mailto:leave-avertalert-131596T@listserv.nai.com)

---

You are currently subscribed to avertalert as: [smueller@symantec.com](mailto:smueller@symantec.com)  
To unsubscribe send a blank email to [leave-avertalert-131596T@listserv.nai.com](mailto:leave-avertalert-131596T@listserv.nai.com)



Sample 3 - More detailed information are published at [http://vil.nai.com/vil/content/v\\_100142.htm](http://vil.nai.com/vil/content/v_100142.htm) on the AVERT web site.

### 3.4 - CERT Coordination Center (web-based)

The CERT Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute at the Carnegie Mellon University.

The information ranges from protecting systems against potential problems to reacting to current problems to predicting future problems. The work involves

- handling computer security incidents and vulnerabilities
- publishing security alerts
- researching long-term changes in networked systems
- developing information and training

to help improve security.

CERT/CC alerts users to potential threats to the security of their systems and provide information about how to avoid, minimize, or recover from the damage. Users are CERT/CCs primary source of information. User's reports help CERT/CC to inform other users about threats and ways to avoid or recover from them.

This is a section of a CERT Advisory:

CERT Advisory CA-2003-12 Buffer Overflow in Sendmail  
Original release date: March 29, 2003  
Last revised: April 1, 2003  
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected  
Sendmail Pro (all versions)  
Sendmail Switch 2.1 prior to 2.1.6  
Sendmail Switch 2.2 prior to 2.2.6  
Sendmail Switch 3.0 prior to 3.0.4  
Sendmail for NT 2.X prior to 2.6.3  
Sendmail for NT 3.0 prior to 3.0.4  
Systems running open-source sendmail versions prior to 8.12.9, including UNIX and Linux systems

#### Overview

There is a vulnerability in sendmail that can be exploited to cause a denial-of-service condition and could allow a remote attacker to execute arbitrary code with the privileges of the sendmail daemon, typically root.

#### I. Description

There is a remotely exploitable vulnerability in sendmail that could allow an attacker to gain control of a vulnerable sendmail server. Address parsing code in sendmail does not adequately check the length of email addresses. An email message with a specially

crafted address could trigger a stack overflow. This vulnerability was discovered by Michal Zalewski.

This vulnerability is different than the one described in CA-2003-07.

Most organizations have a variety of mail transfer agents (MTAs) at various locations within their network, with at least one exposed to the Internet. Since sendmail is the most popular MTA, most medium-sized to large organizations are likely to have at least one vulnerable sendmail server. In addition, many UNIX and Linux workstations provide a sendmail implementation that is enabled and running by default.

This vulnerability is message-oriented as opposed to connection-oriented. That means that the vulnerability is triggered by the contents of a specially-crafted email message rather than by lower-level network traffic. This is important because an MTA that does not contain the vulnerability will pass the malicious message along to other MTAs that may be protected at the network level. In other words, vulnerable sendmail servers on the interior of a network are still at risk, even if the site's border MTA uses software other than sendmail. Also, messages capable of exploiting this vulnerability may pass undetected through many common packet filters or firewalls.

This vulnerability has been successfully exploited to cause a denial-of-service condition in a laboratory environment. It is possible that this vulnerability could be used to execute code on some vulnerable systems.

The CERT/CC is tracking this issue as VU#897604. This reference number corresponds to CVE candidate CAN-2003-0161.

For more information, please see

<http://www.sendmail.org>  
<http://www.sendmail.org/8.12.9.html>  
<http://www.sendmail.com/security/>

For the latest information about this vulnerability, including the most recent vendor information, please see

<http://www.kb.cert.org/vuls/id/897604>  
This vulnerability is distinct from VU#398025.

## II. Impact

Successful exploitation of this vulnerability may cause a denial-of-service condition or allow an attacker to gain the privileges of the sendmail daemon, typically root. Even vulnerable sendmail servers on the interior of a given network may be at risk since the vulnerability is triggered by the contents of a malicious email message.

## III. Solution

Apply a patch from Sendmail Inc.

Sendmail has produced patches for versions 8.9, 8.10, 8.11, and 8.12. However, the vulnerability also exists in earlier versions of the code; therefore, site administrators using an earlier version are encouraged to upgrade to 8.12.9. These patches, and a signature file, are located at

<ftp://ftp.sendmail.org/pub/sendmail/prescan.tar.gz.uu>  
<ftp://ftp.sendmail.org/pub/sendmail/prescan.tar.gz.uu.asc>

Apply a patch from your vendor

Many vendors include vulnerable sendmail servers as part of their software distributions. We have notified vendors of this vulnerability and recorded the statements they provided in Appendix A of this advisory. The most recent vendor information can be found in the systems affected section of VU#897604.

Enable the RunAsUser option

There is no known workaround for this vulnerability. Until a patch can be applied, you may wish to set the RunAsUser option to reduce the impact of this vulnerability. As a good general practice, the CERT/CC recommends limiting the privileges of an application or service whenever possible.

**Sample 4 - Source:** The complete sample of the CERT Advisory CA-2003-12 concerning Buffer Overflow in Sendmail is published at <http://www.cert.org/advisories/CA-2003-12.html> on the vulnerability, incidents and fixes section at the CERT website.

### 3.5 - Symantec Security Response (web-based)

The Symantec Security Response teams are poised to protect organizations from attacks. Through a worldwide network of researchers and technicians working 24//365, Symantec Security Response is

- alerting customers
- creating and distributing fixes to security threats and vulnerabilities
- providing global technical and emergency support

Detailed information about viruses and Vulnerabilities are available at the Symantec Security Response web site.

This is a section of a Symantec Security Response online virus write-up:

W32.FunLove.4099

W32.FunLove.4099 replicates under Windows 95/98/Me and Windows NT. It infects programs that have .exe, .scr, and .ocx extensions. What is notable about this virus is that it uses a new strategy to attack the Windows NT file security system, and it runs as a service on Windows NT systems.

How FunLove works

Files infected with W32.FunLove.4099 insert the Flcss.exe file into the \Windows\System (Windows 95/98/Me) or \Winnt\System32 (Windows NT) folder. Whenever the 4,608-byte Flcss.exe file can be created, the virus attempts to execute it as a service on computers running Windows NT. If for any reason the service can not be executed, the virus creates a thread inside the infected program. This thread infects local and network drives by searching for Portable Executable (PE) files with .exe, .scr, or .ocx extensions. The thread then executes inside the infected process and the main thread of the program takes control. In most cases, this does not cause any noticeable delays. When the virus can execute itself as a service process under the "FLC" name, other infected programs will try to insert the Flcss.exe file, but will not create a new infection thread. W32.FunLove.4099 is the second virus that runs as a service on Windows NT.

The WNT.RemEx.A (W32.RemoteExplore) virus is very similar in its functions to W32.FunLove.4099, but W32.FunLove.4099 can run on both Windows 95/98 and Windows NT. It is, therefore, considered more successful than WNT.RemEx.A. When the virus runs as a service, it can spread on the local drives, even if no one is logged on. Because of this, the virus can infect files that are normally not accessible after the logon. For example, the virus can infect Explorer.exe on a Windows NT system.

On Windows 95/98 computers, infected programs place the Flcss.exe file in the \System folder and try to execute it as a regular process. If the process cannot be executed, the virus tries to execute the infection thread inside the infected host program.

This virus also attacks the Windows NT file security system. For the virus to attempt the attack, it needs administrative rights in Windows NT Server or Windows NT Workstation during the initial infiltration. Once the Administrator or someone with the equivalent rights logs on, W32.FunLove.4099 has the opportunity to modify the Ntoskrnl.exe file, the Windows NT kernel located in the \Winnt\System32 folder. The virus modifies only two bytes in a security API named SeAccessCheck. W32.FunLove.4099 is then able to give full access to all files to all users, regardless of its original protection, whenever the computer is booted with the modified kernel. This means that a Guest--who has the lowest possible rights on the system--can read and modify all files, including files that are normally accessible only by the Administrator. This is a potential problem, because the virus can spread everywhere, regardless of the actual access restrictions on the particular computer. Furthermore, after the attack, no data can be considered protected from modification by any user.

Unfortunately, the consistency of Ntoskrnl.exe is checked only once during the startup process. The loader, Ntldr, checks Ntoskrnl.exe when it loads into physical memory during startup. If the kernel becomes corrupted, Ntldr is supposed to stop loading Ntoskrnl.exe and display an error message, even before a "blue screen" appears. To avoid this, W32.FunLove.4099 patches Ntldr so that no error messages are displayed, and Windows NT will boot successfully, even if its checksum does not match the original. Since no code checks the consistency of Ntldr itself, the patched kernel will be loaded without notifying the user. Because Ntldr is a hidden, system, and read-only file, W32.FunLove.4099 changes the attributes of it to "archive" before it attempts to patch it. The virus does not change the attribute of Ntldr back to its original value after the patch. FunLove can also infect local and network drives. It enumerates the mapped network drives and infects PE files on those computers. In addition, the Ntoskrnl.exe and Ntldr patch is performed on the network drives. Whenever a computer with sufficient rights maps the System drive of a computer running Windows NT, the virus modifies the kernel and the loader components over the network.

The Ntoskrnl.exe and Ntldr patches are executed by a routine picked up from the Bolzano virus. In fact, more than 50 percent of the virus code shows similarities to the Bolzano virus. It is very likely that the author of these two viruses is the same person.

**Sample 5 - Source:** The complete sample of the Funlove virus write-up is published on <http://www.symantec.com/avcenter/venc/data/w32.funlove.4099.html> at the Symantec Security Response web site.

#### **4. Disadvantages of free alerting services and resources**

Monitoring multiple mailings lists and websites means some disadvantages for a company that must keep their environment up-to-date for security reasons.

Every employee who is responsible for a specific section of the environment has to spend time tracking new security threats, searching through vendor websites for patches and eliminate irrelevant alerts.

Detailed Information from must be read completely in order to be able to understand the effects on own systems.

According to a Symantec survey in 2001, security professionals spend an average of 2.1 hours a day searching for security information.

Information from different sources must be qualified and forward to the people who are responsible for the affected systems. Depending on the most pressing security issues, resources must be prioritized and allocated.

## **5. Symantec DeepSight Alert Services**

DeepSight Alert Services deliver timely, complete and actionable information on vulnerabilities and malicious code with countermeasures to defend against these attacks.

### **5.1 Overview**

DeepSight Alert Services' alerts contain all the information security professionals need to protect their infrastructure from attack

- Summary
- Technical description
- Impacts
- Symptoms
- Mitigation strategies
- Patches and/or workarounds when available

Customers can also specify the exact products and versions for which they wish to receive alerts, as Symantec monitors over 3,400 products from 1,600 vendors with almost 14,000 distinct versions. Symantec is tracking information from over 140 different sources.

The comprehensiveness of the alerts, coupled with the ability to customize what alerts they receive, allows customers to save hours every day they would otherwise spend searching through hundreds of E-mails and web sites for the most recent and relevant vulnerability and malicious code information.

By delivering exactly the information customers want to exactly who needs the information, DeepSight Alert Services bridges the gap between awareness and action. Security professionals can now use the time they were spending on research and instead use it to respond to threats and eliminate their exposure to attack.

### **5.2 - How the Service works and Main Components**

Every day, Analysts search hundreds of security vendor, industry and underground websites and mailing lists, looking for information about possible new vulnerabilities or malicious code.

When they discover information about a vulnerability or malicious code (either new threats or revisions to existing threats) they gather all information related to that new vulnerability or malicious code and create an alert. The analysts issue numerical ratings of the risk, based on a number of factors, to quantify the risk. The DeepSight Alert Services system then automatically sends out the alert to those customers who have configured their systems to receive it.

Configuration of the DeepSight Alert Services product is very easy. Customers configure their account simply by selecting what products to watch, how to be notified and when to be notified.

### **5.3 - Requirements**

At the log-in page, customers enter username and password. The System requirements are Internet Explorer 5.0+ or Netscape Navigator 4.6+ with JavaScript enabled. The browser must support SSL. Adobe Acrobat Reader is needed for viewing reports. A valid E-mail address is needed for receiving reports and alerts.

Optional requirements are a telephone number for receiving voice alerts, a fax number for receiving fax alerts or a SMS enabled phone for receiving SMS alerts.

### **5.4 - Creating Technology Lists**

The first step in configuring DeepSight Alert Services is to create a technology list. Tech Lists give customers the freedom to be as specific or as broad as they want when selecting the products for which they wish to receive alerts.

The criteria windows allow customers to select the level of specificity for the alerts they receive. They can select from the following criteria:

- Category (e.g., Operating Systems) will include all products tracked by Symantec that fall into that functional category
- Vendors (e.g., Microsoft) will include all products by that vendor
- Products (e.g., NT Enterprise Server) will include all version of that product
- Versions (e.g., 4.0 Service Pack 5) of a particular product

There is no limit to the number of tech lists a customer can create; they can create multiple lists (e.g., one for web servers, one for operating systems, one for applications) that correspond to different types of technology or different operational areas within the company, or a single comprehensive list one that includes all products. Customers can

also share tech lists within an enterprise, reducing the amount of time required to deploy DeepSight Alert Services.

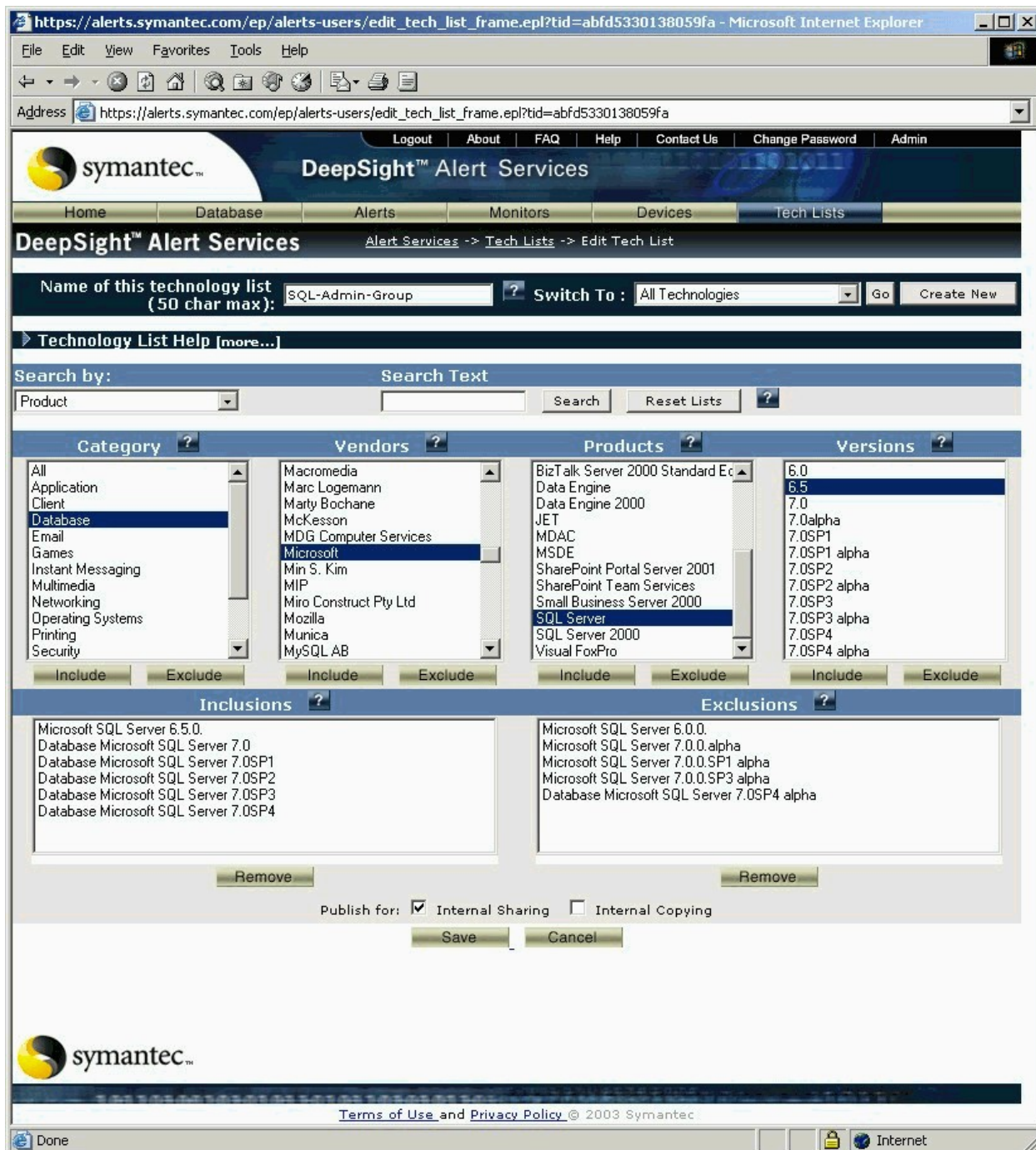


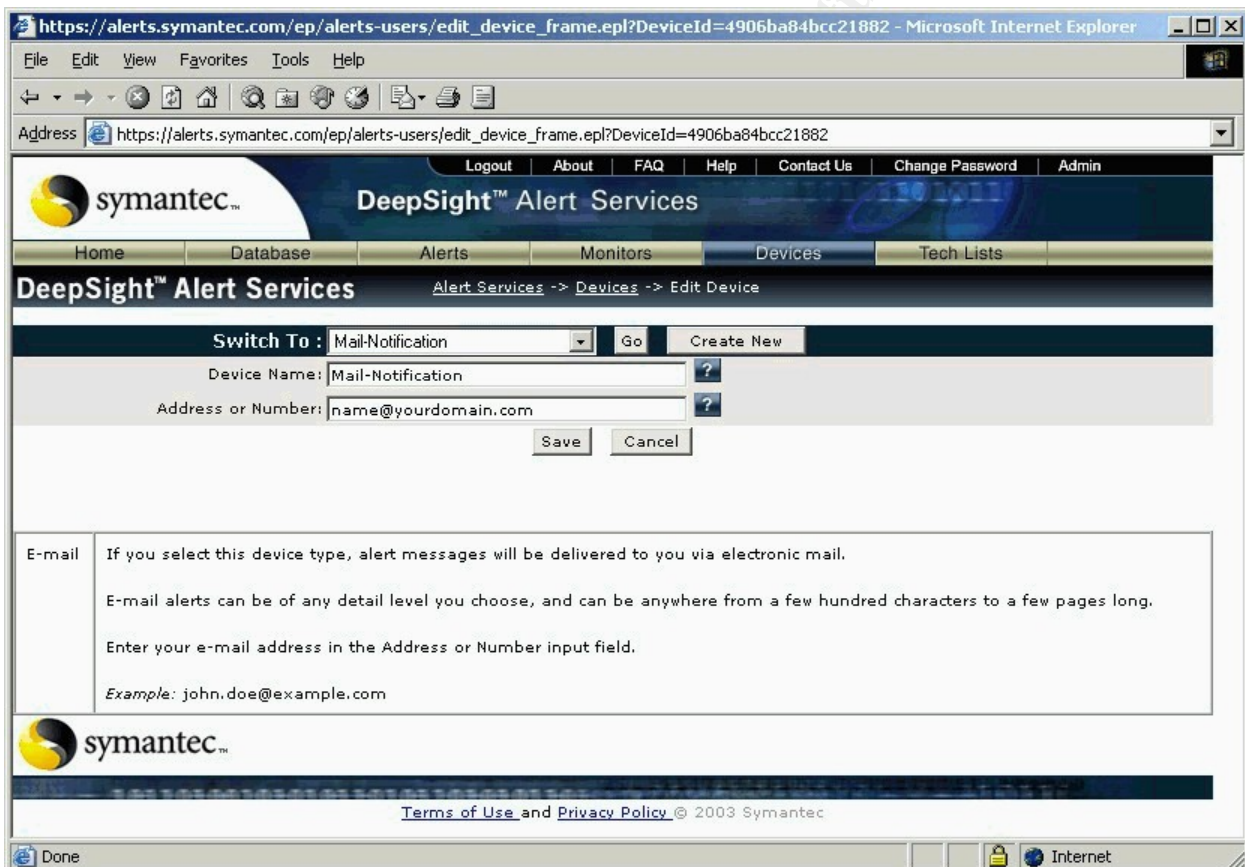
Figure 1 - Symantec DeepSight Alert Service - Tech List

Customers can build tech lists that match their environment exactly, ensuring that they only receive alerts that are applicable to the technology they've deployed. They save time by eliminating alerts that do not apply to their environment, knowing that when they receive an alert it applies to them.

## 5.5 - Configure a Device

The second step in configuring DeepSight Alert Services is to create devices. Devices are the means with which customers receive notifications of alerts. There are four options for notification: E-mail, Fax, SMS and voice. E-mail and fax alerts are full-length; SMS and voice alerts are abbreviated.

To configure a device, give it a name, select what type and then type in the address or number. Customers can create one device per account by default. Additional devices are available for a fee, and there is no limit on the number of additional devices a customer may purchase.



The screenshot shows the Symantec DeepSight Alert Services interface in a Microsoft Internet Explorer browser window. The address bar displays the URL: [https://alerts.symantec.com/ep/alerts-users/edit\\_device\\_frame.epl?DeviceId=4906ba84bcc21882](https://alerts.symantec.com/ep/alerts-users/edit_device_frame.epl?DeviceId=4906ba84bcc21882). The page features a navigation bar with links: Home, Database, Alerts, Monitors, Devices (selected), and Tech Lists. Below the navigation bar, the page title is "DeepSight™ Alert Services" and the breadcrumb trail is "Alert Services -> Devices -> Edit Device".

The main form area includes a "Switch To:" dropdown menu set to "Mail-Notification", a "Go" button, and a "Create New" button. Below this, there are two input fields: "Device Name" (containing "Mail-Notification") and "Address or Number" (containing "name@yourdomain.com"). There are "Save" and "Cancel" buttons at the bottom of the form.

Below the form, there is a section titled "E-mail" with the following text:

- If you select this device type, alert messages will be delivered to you via electronic mail.
- E-mail alerts can be of any detail level you choose, and can be anywhere from a few hundred characters to a few pages long.
- Enter your e-mail address in the Address or Number input field.
- Example: john.doe@example.com

The footer of the page includes the Symantec logo and the text "Terms of Use and Privacy Policy © 2003 Symantec". The browser's status bar at the bottom shows "Done" and "Internet".

Figure 2 - Symantec DeepSight Alert Service - Devices

Being able to configure multiple devices for each account give customers complete flexibility as to how they wish to receive alerts; they can determine how and when they wish to be notified to ensure that they receive their alerts in the most appropriate manner; for example, all alerts delivered via E-mail, and the most urgent alerts delivered via voicemail or SMS.



## 5.6 - Using Monitors to Combine Technology Lists and Devices

The final step in configuring DeepSight Alert Services is to create a monitor. Customers combine tech lists (what to watch) and devices (how to be notified) to create monitors. Monitors allow them to select specific ratings that will determine when and how they receive alerts.

Customers create their custom alert strategy by selecting when an alert for one or more tech lists will be sent to a device. Each alert sent by Symantec has ratings for urgency, impact and other measures, depending on whether it is a vulnerability or malicious code. These ratings allow customers to create a response and notification escalation strategy within their organization.

For example, a customer can create one monitor that has all vulnerability alerts for a tech list with an urgency rating of 3 to go to E-mail; all alerts for the same tech list with an Urgency above a 7 to go to SMS, and all alerts 9 or higher to go to their mobile phone. Another example is for the Director of IT to have a Monitor that all malicious code alerts for all Tech Lists with an urgency rating of 8 or higher to go to voicemail, ensuring that she receive immediate notification of all critical alerts.

There are four steps to configuring a monitor are

- Monitor options – choose whether to create a malicious code or vulnerability monitor
- Monitor settings – select the name of the monitor and the thresholds to determine when an alert is sent
- Choose technology list – pick the technology to which the thresholds will apply
- Choose device – choose which device will receive the alerts matching the threshold(s) and tech list(s)

Threshold settings give customers the ability to customize when an alert for a tech list gets sent to a device by choosing a rating threshold. For vulnerability alerts they can specify urgency, impact & credibility (malicious code alerts have urgency and impact thresholds).

Each monitor is unique to each customer; they determine when they will receive an alert by selecting the threshold(s) with which they're concerned. The more thresholds selected, or the more restrictive a threshold (i.e., the higher the numerical rating) the fewer alerts will be sent. Customers therefore have complete control over what they receive, based on their own criteria.

## 5.7 - View Alerts and the Database Page

The Alerts Page gives customers the ability to view all the alerts they've received from any web browser. They can choose to view all alerts, or just vulnerability or malicious code alerts individually.

The screenshot shows the Symantec DeepSight Alert Services web interface. The page title is "Listing Sent Alerts - Microsoft Internet Explorer". The address bar shows "https://alerts.symantec.com/ep/alerts-users/sent\_alerts.epl". The page has a navigation bar with links: Home, Database, Alerts, Monitors, Devices, Tech Lists. The main content area is titled "DeepSight™ Alert Services" and "Alert Services -> Sent Alerts".

Below the navigation bar, there is a search and filter section. It includes a "Date Range" selector (2003, Apr, 07 To 2003, Apr, 07), a "Results Per Page" selector (15), a "Monitor" dropdown (All Monitors), and a "Status" dropdown (All). There are "Search" and "Reset Search" buttons.

The main table is titled "Received Alerts" and contains the following data:

| Date (GMT)          | Type                   | Devices (Addresses) | Monitors            | ID    | Title                                                             | Status         |
|---------------------|------------------------|---------------------|---------------------|-------|-------------------------------------------------------------------|----------------|
| Apr 07 2003 11:43PM | Vulnerability          | Symantec @ .com)    | Vulnerability Alert | 7294  | Samba 'call trans2open' Remote Buffer Overflow Vulnerability      | Resolved       |
| Apr 07 2003 09:55PM | Vulnerability          | Symantec @ .com)    | Vulnerability Alert | 7295  | Samba Multiple Unspecified Remote Buffer Overflow Vulnerabilities | Resolved       |
| Apr 07 2003 07:51PM | Vulnerability          | Symantec @ .com)    | Vulnerability Alert | 7295  | Samba Multiple Unspecified Remote Buffer Overflow Vulnerabilities | In Progress    |
| Apr 07 2003 06:07PM | Vulnerability          | Symantec @ .com)    | Vulnerability Alert | 7294  | Samba 'call trans2open' Remote Buffer Overflow Vulnerability      | Unresolved     |
| Apr 07 2003 05:08PM | Vulnerability          | Symantec @ .com)    | Vulnerability Alert | 7294  | Samba 'call trans2open' Remote Buffer Overflow Vulnerability      | Unresolved     |
| Apr 07 2003 04:20PM | Vulnerability          | Symantec @ .com)    | Vulnerability Alert | 7112  | Linux Kernel Privileged Process Hijacking Vulnerability           | Unresolved     |
| Apr 07 2003 04:12PM | Analyst Incident Alert | Symantec @ .com)    | Incident Alert      | 1228  | Analyst Incident Alert                                            | In Progress    |
| Apr 07 2003 03:49PM | ThreatCon              | Symantec @ .com)    | ThreatCon Monitor   | 11610 | ThreatCon                                                         | Unresolved     |
| Apr 07 2003 03:29PM | Vulnerability          | Symantec @ .com)    | Vulnerability Alert | 7294  | Samba 'call trans2open' Remote Buffer Overflow Vulnerability      | Unresolved     |
| Apr 07 2003 02:40PM | Vulnerability          | Symantec @ .com)    | Vulnerability Alert | 7294  | Samba 'call trans2open' Remote Buffer Overflow Vulnerability      | Unresolved     |
| Apr 07 2003 06:35AM | Analyst Report (Daily) | Symantec @ .com)    | Daily Reports       | 1227  | Analyst Report (Daily)                                            | Not Applicable |

At the bottom of the table, it says "11 records matched" and "page 1 of 1". There is a "Jump to page" dropdown set to "1" and a "GO" button.

The footer of the page includes the Symantec logo and the text "Terms of Use and Privacy Policy © 2003 Symantec".

Figure 3 - Symantec DeepSight Alert Service - Alerts

A additional Database page gives customers access to every vulnerability and malicious code alert issued by Symantec. Customers can sort by Bugtraq ID (BID) or Malicious Code ID (MCID), last update and original publish date. They can search by description, title, vendor and product.

- The Alerts page gives customers access to their alerts from anywhere in the world, at any time. If they are out of the office, they do not have to rely on gaining access to their E-mail application or internal applications to view the alert and respond to the threat
- The Database page allows customers to research technologies in their environment for previous alerts, as well as search for prior alerts on products for which they may be interested

## 5.8 - The Alert Notification from DeepSight

Symantec DeepSight Alert Services deliver timely notification, enabling enterprises to better protect critical information assets. Customers receive alerts on new vulnerabilities and malicious code. They get comprehensive vulnerability and malicious code information, covering all of the customer's systems. All alerts are specific to each customer's technologies. The alerts include complete vulnerability and malicious code analysis, along with effective attack mitigation strategies and detailed patch information.

This is a sample of a DeepSight Alert Notification concerning a Apple QuickTime Player vulnerability:

```

 Security Alert

Subject: Apple QuickTime Player Custom URL Vulnerability
BUGTRAQ ID: 7247 CVE ID: CAN-2003-0168
Published: 2003-03-31 Updated: 2003-03-31 22:59:08 GMT

Remote: Yes Local: No
Availability: User Initiated Authentication: Not Required
Credibility: Vendor Confirmed Ease: No Exploit Available
Class: Boundary Condition Error

Impact: 9.0 Severity: 8.9 Urgency: 7.5

Last Change: Initial analysis.

Vulnerable Systems:

 Apple QuickTime Player 5.0.2
 Apple QuickTime Player 6

Non-Vulnerable Systems:

 Apple QuickTime Player 6.1

Short Summary:
```

Apple QuickTime Player for Microsoft Windows vulnerable to an issue that could allow code execution if a malicious URL is loaded into the player.

#### Impacts:

It is possible to execute arbitrary code as the user of a QuickTime Player.

#### Technical Description:

QuickTime Player is the media player distributed by Apple for QuickTime Media Files. This problem affects the player on the Microsoft Windows platform.

A problem in the software may make remote code execution possible.

It has been reported that the QuickTime Player does not properly handle some types of URLs. Because of this, a remote attacker may be able to execute arbitrary commands on the vulnerable system.

Few technical details are available concerning this vulnerability. It is known that for an attack to be successful, a user must load a maliciously-crafted URL into the QuickTime Player. It is also known that loading the URL results in the execution of arbitrary code as the QuickTime user.

Initial reports indicate that this issue is a buffer overrun vulnerability. If this is the case, it would be possible for the attacker to place malicious instructions in the URL supplied to the target user. When the URL is loaded into the player, the instructions contained in the URL would be executed with the privileges of the user invoking QuickTime. This vulnerability has been reported to affect QuickTime on only the Microsoft Windows platform.

#### Attack Scenarios:

To exploit this vulnerability, an attacker must have a means of delivering a malicious URL to the user of a vulnerable QuickTime Player.

An attacker creates a malicious URL, and sends it to a target user via a means such as e-mail.

The victim clicks on the URL which is passed to QuickTime, resulting in the execution of arbitrary code contained in the malicious URL.

#### Exploits:

Currently we are not aware of any exploits for this issue. If you feel we are in error or are aware of more recent information, please mail us at: [deepsightcustserv@symantec.com](mailto:deepsightcustserv@symantec.com) <<mailto:deepsightcustserv@symantec.com>>.

#### Mitigating Strategies:

Do not follow links provided by unknown or untrusted sources.

Do not click on links sent from unknown or untrusted sources. If this is not possible, visit links as a restricted user with minimal access privileges.

Deploy network intrusion detection systems to monitor network traffic for malicious activity.

Use intrusion detection systems to monitor network traffic for attempted attacks, and alert personnel responsible for security to threats.

#### Solutions:

Apple has stated that this vulnerability has been fixed in QuickTime 6.1. It can be downloaded by either using the "Update Existing Software..." option in the QuickTime Help menu, or from the following URL:

<http://www.apple.com/quicktime/download/>

For Apple QuickTime Player 5.0.2:

Apple Upgrade QuickTime Player 6.1

<http://www.apple.com/quicktime/download/>

For Apple QuickTime Player 6:

Apple Upgrade QuickTime Player 6.1

<http://www.apple.com/quicktime/download/>

#### Credit:

Discovery is credited to Texonet.

#### References:

web page:

Apple Security Updates (Apple)

[http://www.info.apple.com/usen/security/security\\_updates.html](http://www.info.apple.com/usen/security/security_updates.html)

#### ChangeLog:

Mar 31, 2003: Initial analysis.

#### URL:

<https://alerts.symantec.com/view/bid/237b4721dec39a82>

Report Created: 2003-04-01 03:47:35 GMT

Copyright 2003 Symantec.com

For help with interpreting the meaning of any of the sections or labels

in this alert, please visit:  
<https://alerts.symantec.com/help/sia-users/vulnerability-alert-text.htm>

This alert was triggered by the monitor: Vulnerability Alert  
This device is named: Symantec

Symantec Corporation  
The World Leader in Internet Security Technology and Early Warning Solutions  
Visit our website at [www.symantec.com](http://www.symantec.com)

View public key at:  
<http://alerts.symantec.com/Profiles/SecurityFocus/ep/alerts-users/gnupg-sigkey.ep1>

## Sample 6 - E-mail notification from Symantec DeepSight Alert Services

### 5.9 - How To license Symantec DeepSight Alert Services

Symantec licenses Symantec DeepSight Alert Services in one or two-year subscriptions, based on the

- Number of user seats required for an organization
- Delivery options selected

A user seat represents an individual subscriber with authorization to access the web service, query the vulnerability database, configure alerts, and receive E-mail alerts. Customers can choose to deliver alerts to additional devices or contacts within their organization for an additional fee. Add-on delivery options include Fax, SMS, Voice and E-mail.

### 6. Benefits of a commercial alerting service

By providing notification of new potential threats as they're identified, with detailed, actionable information, Symantec DeepSight Alert Services helps administrators mitigate vulnerabilities before they can be exploited, and helps protect systems from malicious code before it strikes.

#### Symantec DeepSight Alert Services

- provides alerts only for vulnerabilities on systems, networks, and technologies deployed in a customers' environment
- delivers alerts directly to the IT manager responsible for maintaining the specific application, system, or network
- reduces time spent tracking new security threats
- eliminates the need to monitor multiple mailings lists/Web sites or to sift through irrelevant alerts

- ensures the information goes directly to the people with the skill and ability to recognize and fix the security vulnerability before it can be exploited

Symantec DeepSight Alert Services provides a complete analysis of each vulnerability and malicious code, including

- the severity of each vulnerability or malicious code
- source credibility
- the systems and versions affected
- technical description of the threat
- mitigation strategies
- impact and symptoms
- workarounds and available patches

Alerts are delivered through E-mail, fax, SMS or voice, configurable according to the urgency of the threat.

The service provides all the information customers need to take action and to defend their resources and enables them to deploy countermeasures and to thwart attacks before they hit. It eliminates the time spent searching through vendor sites for corrective downloads and helps to prioritize and allocate resources.

A commercial service like Symantec DeepSight Alert Services helps ensure customers get the information they need, the way they need it and enables them, for example, to better allocate staff time and resources, based on the most pressing security issues.

## 7. Sources Cited/Referenced

- CERT Advisory Mailing List  
[http://www.cert.org/contact\\_cert/certmaillist.html](http://www.cert.org/contact_cert/certmaillist.html)
- CERT Coordination Center (CERT/CC)  
<http://www.cert.org/nav/index.html>
- Cisco Systems Technical Assistance Center (TAC) Newsletter  
<http://tools.cisco.com/RPF/register/register.do>
- McAfee AVERT (Anti-Virus Emergency Response Team)  
<http://www.mcafeeb2b.com/naicommon/avert/>  
<http://vil.nai.com/vil/content/alert.htm>
- Microsoft Security Update  
<http://register.microsoft.com/subscription/subscribeme.asp?id=166>
- Microsoft Security Notification Service (Microsoft Passport Required)

<http://register.microsoft.com/regsys/pic.asp>

- SANS Institute - Critical Vulnerability Analysis Newsletter  
<https://server2.sans.org/sansnews>

- Symantec Mailing Lists  
<http://www.Symantec.com/cgi-bin/sfonline/subscribe.pl>

- Symantec Internet Security Threat Report Volume III  
<http://enterprisesecurity.symantec.com/Content.cfm?articleID=1964&EID=0>

- Symantec DeepSight Alert Services  
<http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=160&EID=0>

- Symantec DeepSight Threat Management System  
<http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=158&EID=0>

- Symantec Security Response  
<http://www.symantec.com/avcenter/>

© SANS Institute 2003, Author retains full rights.