Global Information Assurance Certification Paper

Internet Explorer Web Browser Security Review

SANS GSNA V3.2
Practical Assignment

Jim Govekar
September 19, 2004

Abstract

In the world of the "World Wide Web" the web browser has become a necessary tool in the workplace to conduct business, do research, and to share information. Web browsers are the client applications that communicate with web servers.
The web browser is also a tool that can be used by malicious individuals to exploit vulnerabilities on various personal computers.

In this paper, I will address the audit process to review the Microsoft Internet Explorer web browser for potential vulnerabilities that could result in compromise of valuable data such as financial information, personal data, or company sensitive information. The primary browser that is used in the fictitious company, JG Systems, is Microsoft's Internet Explorer version 6. As with any process, the audit objective is to establish an accurate, repeatable process that will provide value to our customers. The goal of this paper is to provide a detailed description of the necessary steps required to meet the auditing objective and to provide the reader with a practical example of what is required to conduct the audit of web browsers.

Table of Contents

Part 1: Identification of Subject and Risks

If you sit down at any personal computer you will probably find a web browser installed on the machine. Many of these browsers are installed as a standard feature of the operating system or are available free for download from the internet. The fictitious company that is being audited for this assignment, JG Systems, has decided to use Microsoft's Internet Explorer as their browser of choice.

This audit will take a look at the security of the web browsers of JG Systems. Since the company has an active connection to the internet and employs staff with the capability of accessing the web as part of their normal duties, a review of the browsers is being done to try and limit the potential vulnerabilities that can be caused by improper settings.

The increase of web sites and the associated easy access to information have made web browsers critical business applications. As with other widely available, highly used software products, the web browser has become a common target for malicious individuals trying to disrupt business processes.

Some commonly used attacks:

- Mobile Code contained in data that is sent to the browser can cause:
  - Damaged files on the client computer.
  - Permanent data loss.
  - Disclosure of data stored on the client.
  - Denial of Service attacks.

Software Maintenance

According to the DISA Desktop Application STIG, maintaining the security of web browsers requires frequent reviews of security bulletins. Many security bulletins mandate the installation of a software patch to overcome security vulnerabilities. System Administrators should regularly check browser vendor web sites for information on new security patches that are applicable to their site. All applicable security patches will be applied to the system. A security patch is deemed applicable if the product is installed, even if it is not used or is disabled.

Software vendors are offering services that provide for automatic installation of patches. These services can assist the system administrator with keeping up to date with the various patches the vendor is distributing. It is recommended that these automatic services be controlled and monitored by the system administrators to prevent the installation of un-approved software.

Secure Browser Communication

Safe communications between browser and server is critical to the use of the browser in business and for the personal user. The use of Secure Socket Layer (SSL) is the standard means used to address the security of this traffic. SSL provides the user with encryption capabilities for data in transport and the digital certificates that are installed on the web server provide assurance to the user of the authenticity of the site. Most of the commercial browsers support Versions 2 and 3 of SSL.

Mobile Code

Software is transferred from one computer, such as a web server, to a client computer with the objective to be executed on the client, is what is known as Mobile Code. Not all mobile code is malicious by design, some result is negative consequences due to poor design and testing of legitimate code, some works just as designed and causes no problems, but some work as designed and can destroy a system or compromise sensitive data without the knowledge of the user. Since the web browser is a primary host for the execution of mobile code, it is critical to configure the parameters that impact mobile code execution. The following provides examples of mobile code:

- ActiveX
- Shockwave
- Java Applets
- Visual Basic for Applications (VBA)
- LotusScript
- PerfectScript
- Postscript
- Javascript
- VBScript
- Portable Document Format (PDF)
- Flash

Current state of the practice

As part of the research for this project, I found many sites that provided information about the web in general and some with specifics for the web browser. Although this paper is primarily focused on Microsoft's Internet Explorer, many of the sites presented information on the other major browsers such ad Mozilla, and Netscape Navigator.

The Central Arizona College provided detailed information about many of the settings for Internet Explorer 6.0.

http://www.centralaz.edu/inetclasses/setup/IE-Complete-Settings.htm

The University of Maryland University College web site addressed issues with many of the web browser settings.

http://www.umuc.edu/library/database/browser.html

The Penn Computing site general information about the web and provided some information on the securing of the desktop environment.

http://www.upenn.edu/computing/security/checklists/desktop.html

The Microsoft web site has extensive information about the Internet Explorer web browser. It identifies many of the vulnerabilities that exist in IE and provides direction on remediation of these vulnerabilities. A sample of the links is included.

http://www.microsoft.com/technet/security/chklist/iecl.mspx

http://www.microsoft.com/resources/documentation/ie/6/all/reskit/en-us/part7/z04ie6rk.mspx

The National Security Agency has published many guides on the security of many operating systems and application products.

Guide to Securing Windows NT/9x Clients in a Windows 2000 Network

Part 2: Create an Audit Checklist

IE001 Internet Explorer Version

Description:	The installed version of IE is not current
Reference:	Personal Experience www.cert.org www.microsoft.com Defense Information Systems Agency – Desktop Application Security Technical Implementation Guide
Risk:	Versions of Internet Explorer 5.5 without Service Pack (SP) 2 have known significant security vulnerabilities. This includes privilege-elevation and information disclosure vulnerabilities. Subsequent security patches require SP2 to be installed. Versions of Internet Explorer 6.0 without Service Pack (SP) 1 have known significant security vulnerabilities. This includes privilege-elevation and information disclosure vulnerabilities. Subsequent security patches require SP1 to be installed.
Testing Procedure:	Procedure: Search for the shdocvw.dll file using Windows Explorer or the Start menu "Search | For Files or Folders…" facility Determine the version of the shdocvw.dll file. Criteria: The version number of the shdocvw.dll file needs to be: 6.00.*x.y*, and the value of x is greater than 28000 or 5.50.*x.y* and the value of x is greater than 4807
Test Nature:	Objective
Evidence:	
Finding:	

IE002 Internet Explorer Internet Options Settings

Description:	Improper IE Options
Reference:	Personal Experience National Security Agency - Security Recommendation Guides Defense Information Systems Agency – Desktop Application Security Technical Implementation Guide
Risk:	If the specified Internet Options are not configured as required, availability and information disclosure vulnerabilities can arise. If options restricting software updates are not enabled, malicious code could be introduced into the client environment. If options restricting the assignment of web sites to privileged IE Security Zones are not properly configured; malicious sites may be able to invoke programs intended for use only by trusted sites. If options that enable stronger session protocols are disabled, information sent over SSL sessions may be more vulnerable to interception. If options related to session encryption warnings are not enabled, a user may unintentionally send sensitive information over a non-encrypted session.
Testing Procedure:	Procedure: Start Internet Explorer On the Tools menu, select the Internet Options a) On the Internet Options window, select the Security tab. Select the icons for the Internet zone, the Local intranet zone, the Trusted sites zone, and the Restricted sites zone to determine if the Security level is Custom for each one. b) Select the Security tab and the Local intranet zone. Select the Sites button. Determine if any of the Include all options are enabled. c) [For IE version 6] Select the Privacy tab and determine the Settings value. d) Select the Advanced tab. Determine the settings for the options in IE Advanced Options Table listed following this check.

	Criteria: All Security levels need to be set to Custom for <u>all</u> of the zones None of the "Include all" options are enabled [For IE version 6] The Privacy Settings value must be at Medium High, High, or Block All Cookies Advanced options are not set as in accordance with the IE Advanced Options Settings Table
Test Nature:	Objective
Evidence:	
Finding:	

IE ADVANCED OPTIONS SETTINGS Table	
PARAMETER	**SETTING**
Automatically check for Internet Explorer updates	Disable
Enable Install On Demand (Internet Explorer - [IE 6.0 only])	Disable
Enable Install On Demand (Other) [IE 6.0 only]	Disable
When searching	Do not search from the Address bar [or] Just display the results in the main window [or] [No option selected]
Check for signatures on downloaded programs [IE 6.0 only]	Enable
Use Private Communication Technology (PCT)1.0 [IE 5.5 only]	Disable
Use SSL 3.0	Enable
Use TLS 1.0	Enable
Warn about invalid site certificates	Enable
Warn if changing between secure and not secure mode	Enable
Warn if forms submittal is being redirected	Enable

IE003 Temporary Internet File Folder Access Control

Description:	Access to a user's Temporary Internet files folder is not restricted properly.
Reference:	Personal Experience National Security Agency - Security Recommendation Guides Defense Information Systems Agency – Desktop Application Security Technical Implementation Guide
Risk:	If web pages displayed during an encrypted (SSL) session are cached in users Temporary Internet files folder and access to that folder is not properly restricted, an information disclosure vulnerability exists. Third parties with access to a users Temporary Internet files folder may be able to recover sensitive data sent during an encrypted browser session.
Testing Procedure:	Procedure: Start Internet Explorer On the Tools menu, select the Internet Options a) On the Internet Options window, determine if the Advanced tab is present. b) If the Advanced tab is not present, it is necessary to use the Windows Registry Editor. Navigate to the following key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings. If the value data for the DisableCachingOfSSLPages value name is 1 (the number one), the Do not save encrypted pages to disk option is enabled. c) If the Advanced tab is present, select it. Determine the value of the Do not save encrypted pages to disk option. d) If the Do not save encrypted pages to disk option is not enabled, select the General tab on the Internet Options window. On the General tab, select the Settings… button. On the Settings… window, determine the folder name specified in the Current location: setting. Criteria: The Do not save encrypted pages to disk option is not enabled and the permissions of the Temporary Internet files folder are not the same as, or more restrictive than, those in the following table

	<table><tr><th>Object Name</th><th>Account Assignment</th><th>Permission</th></tr><tr><td>*variable*\Temporary Internet Files (The *variable* portion of the path name depends on the configuration setting in Internet Explorer.)</td><td>Administrators CREATOR OWNER SYSTEM [*user*]</td><td>all all all all</td></tr></table>
Test Nature:	Objective
Evidence:	
Finding:	

IE004 IE Advanced Internet Options Access Control

Description:	The Advanced settings in the IE Internet Options can be changed by users.
Reference:	Personal Experience National Security Agency - Security Recommendation Guides Defense Information Systems Agency – Desktop Application Security Technical Implementation Guide
Risk:	If users are able to change the Internet Options Advanced settings, availability and information disclosure vulnerabilities can arise. Information disclosures may occur as the result of weakened security settings that no longer restrict data access. Client availability and data integrity issues can result from settings that allow malicious code to execute.
Testing Procedure:	Procedure: Start Internet Explorer On the Tools menu, select the Internet Options a) On the Internet Options window, determine if the Advanced tab is present. b) If the Advanced tab is present, select it. Determine if the options can be changed by attempting to enable or disable a non-sensitive option such as Always expand ALT text for images. Always select the Cancel button to close the Internet Options window.

	Criteria: If the Advanced tab is present and it is possible for a user to change an option.
Test Nature:	Objective
Evidence:	
Finding:	

IE005 IE Security Zone Settings

Description:	The IE Security Zones options are not configured as required.
Reference:	Personal Experience National Security Agency - Security Recommendation Guides Defense Information Systems Agency – Desktop Application Security Technical Implementation Guide
Risk:	If the specified Security Zones settings are not configured as required, availability and information disclosure vulnerabilities can arise. If options restricting the execution of ActiveX controls are not properly configured, malicious code could be executed in the client environment. If options restricting downloads and other types of data flow are not properly configured, malicious code could be introduced into the client environment and client data could be disclosed. If options restricting the execution of Java applets are not properly configured, malicious code could be executed in the client environment. If options related to session encryption warnings are not enabled, a user may unintentionally send sensitive information over a non-encrypted session.
Testing Procedure:	Procedure: Start Internet Explorer On the Tools menu select the Internet Options If the Security tab is present, select it.

	a) Select the Internet icon. If the Custom level… button is enabled, select it. On the Security Settings window, determine the settings for the options indicated in the Security Zone Table. Always select the Cancel button to close the Security Settings window. b) Select the Local intranet icon. If the Custom level… button is enabled, select it. On the Security Settings window, determine the settings for the options indicated in the Security Zone Table. Always select the Cancel button to close the Security Settings window. c) Select the Trusted sites icon. If the Custom level… button is enabled, select it. On the Security Settings window, determine the settings for the options indicated in the Security Zone Table. Always select the Cancel button to close the Security Settings window. d) Select the Restricted sites icon. If the Custom level button is enabled, select it. On the Security Settings window, determine the settings for the options in the Security Zone Options table. Always select the Cancel button to close the Security Settings window. If the Security tab is not present or if the Custom level button is not enabled, the checks can only be performed using the Windows Registry Editor. Navigate to the following keys: HKCU\Software\Microsoft\Windows\CurrentVersion\InternetSettings\Zones*n*, Where *n* is 1 for Local intranet, 2 for Trusted sites, 3 for Internet, and 4 for Restricted sites. Determine the settings for the values in Zone Table Criteria: The Security Settings options in any of the zones must be set as indicated in, or more restrictively than indicated in the Security Zone Table
Test Nature:	Objective
Evidence:	
Finding:	

IE SECURITY ZONE OPTIONS SETTINGS				
PARAMETER	INTERNET ZONE	LOCAL INTRANET ZONE	TRUSTED SITES ZONE	RESTRICTED SITES ZONE
Download signed ActiveX controls	Disable	Prompt		Disable
Registry value: 1001	0x3	0x1		0x3
Download unsigned ActiveX controls	Disable	Disable		Disable
Registry value: 1004	0x3	0x3		0x3
Initialize and script ActiveX controls not marked as safe	Disable	Disable		Disable
Registry value: 1201	0x3	0x3		0x3
Run ActiveX controls and plug-ins	Prompt	Prompt		Disable
Registry value: 1200	0x1	0x1		0x3
Script ActiveX controls marked safe for scripting	Prompt	Prompt		Disable
Registry value: 1405	0x1	0x1		0x3
Allow cookies that are stored on your computer [IE 5.5 only]	Prompt	Enable		Disable
Registry value: 1A02	0x1	0		0x3
Allow per-session cookies (not stored) [IE 5.5 only]	Prompt	Enable		Disable
Registry value: 1A03	0x1	0		0x3
File download	Enable	Enable		Disable
Registry value: 1803	0	0		0x3
Font download	Prompt	Enable		Disable
Registry value: 1604	0x1	0		0x3
Java permissions	Disable Java [Preferred] [or] Custom	Custom		Disable Java
Registry value: 1C00	0 [or] 0x800000	0x800000		0
Access data sources across domains	Disable	Prompt		Disable
Registry value: 1406	0x3	0x1		0x3
Allow META REFRESH [IE 6.0 only]	Enable	Enable		Disable
Registry value: 1608	0	0		0x3
Display mixed content [IE 6.0 only]	Prompt	Enable		Disable
Registry value: 1609	0x1	0		0x3
Don't prompt for client certificate selection when no certificate or only one certificate exists	Disable	Disable		Disable
Registry value: 1A04	0x3	0x3		0x3

Drag and drop or copy and paste files	Prompt	Prompt	Disable
Registry value: 1802	0x1	0x1	0x3
Installation of desktop items	Disable	Prompt	Disable
Registry value: 1800	0x3	0x1	0x3
Launching programs and files in an IFRAME	Disable	Prompt	Disable
Registry value: 1804	0x3	0x1	0x3
Navigate sub-frames across different domains	Prompt	Enable	Disable
Registry value: 1607	0x1	0	0x3
Software channel permissions	High safety	High safety	High safety
Registry value: 1E05	0x10000	0x10000	0x10000
Submit non-encrypted form data	Prompt	Enable	Disable
Registry value: 1601	0x1	0	0x3
User data persistence	Disable	Enable	Disable
Registry value: 1606	0x3	0	0x3
Active scripting	Enable	Enable	Disable
Registry value: 1400	0	0	0x3
Allow paste operations via script	Disable	Prompt	Disable
Registry value: 1407	0x3	0x1	0x3
Scripting of Java applets	Prompt	Enable	Disable
Registry value: 1402	0x1	0	0x3
User Authentication – Logon	Prompt for user name and password	Prompt for user name and password	Anonymous logon
Registry value: 1A00	0x10000	0x10000	0x30000

IE006 IE Security Zone Settings Access Control

Description:	The Security Zone settings or assigned sites in the IE Internet Options can be changed by users.
Reference:	Personal Experience Defense Information Systems Agency – Desktop Application Security Technical Implementation Guide
Risk:	If users are able to change the Internet Options Security Zone settings, availability and information disclosure vulnerabilities can arise. Information disclosures may occur as the result of weakened security settings that no longer restrict data access. Client availability and data integrity issues can result from settings that allow malicious code to execute.
Testing Procedure:	Procedure: Start Internet Explorer On the Tools menu, select the Internet Options On the Internet Options window, determine if the Security tab is present. If the Security tab is present, select it and then the Trusted sites icon. a) If the Custom level button is enabled, select it. On the Security Settings window, determine if the options can be changed by attempting to enable or disable a non-sensitive option such as Font download. Always select the Cancel button to close the Security Settings window. b) Select the Sites button. On the Trusted sites window, determine if it is possible to change the assigned sites by typing into the Add this Web site to the zone: text box. If the Add button becomes enabled, it is possible to change the assigned sites. Always select the Cancel button to close the Trusted sites window. Criteria: If the Security tab is present and it is possible for a user to change any of the zone options or the sites assigned to a zone
Test Nature:	Objective
Evidence:	
Finding:	

IE007 IE Ciphers

Description:	The ciphers enabled for IE SSL sessions allow reduced session security.
Reference:	Personal Experience Defense Information Systems Agency – Desktop Application Security Technical Implementation Guide
Risk:	If the specified SSL cipher options are not configured as required, information disclosure vulnerabilities can arise. The use of null or weaker encryption algorithms could allow intercepted session data to be more easily decrypted.
Testing Procedure:	Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\ SCHANNEL\Ciphers. Look for the DES 56/56, NULL, and Triple DES 168/168 keys and determine the value data for the Enabled value of each key. Criteria: The value data for the Enabled value must be 0 for the NULL key The value data for the Enabled value must be 0xffffffff for the DES 56/56 and the Triple DES 168/168 keys
Test Nature:	Objective
Evidence:	
Finding:	

IE008 IE Hashes

Description:	The hashes enabled for IE SSL sessions allow reduced session security.
Reference:	Personal Experience Defense Information Systems Agency – Desktop Application Security Technical Implementation Guide

Risk:	If the specified SSL hash options are not configured as required, information integrity vulnerabilities can arise. The use of weaker hash algorithms could allow intercepted session data to be more easily modified without detection.
Testing Procedure:	Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\ SCHANNEL\Hashes\SHA Determine the value data for the Enabled value. Criteria: The value data for the Enabled value must be 0xffffffff
Test Nature:	Objective
Evidence:	
Finding:	

IE009 Root CA Certificate for IE

Description:	The required Root Certificate Authority certificate is not installed for IE.
Reference:	Personal Experience Defense Information Systems Agency – Desktop Application Security Technical Implementation Guide
Risk:	If non approved Root Certificate Authority certificates are installed, information disclosure vulnerabilities can result. Web browser sessions may be established with sites impersonating the web site for which a connection was intended. If an unapproved Root Certificate Authority certificate is installed, users may invalidly authenticate a web sites identity and unintentionally allow a session with a counterfeit site.
Testing Procedure:	Procedure: Start Internet Explorer On the Tools menu, select the Internet Options

	On the Internet Options window, select the Content tab and then the Certificates button. On the Certificate Manager window, select the Trusted Root Certification Authorities tab. Scroll through the list of certificates to validate the entries to determine which root CAs are included. Criteria: The entries that are present must be in accordance with company policy.
Test Nature:	Objective
Evidence:	
Finding:	

IE010 IE Error Reporting Tool

Description:	The Error Reporting tool for IE is installed or enabled.
Reference:	Personal Experience Defense Information Systems Agency – Desktop Application Security Technical Implementation Guide
Risk:	If the Error Reporting tool for IE is enabled, an information disclosure vulnerability exists. A user may send sensitive information in a document to Microsoft when an IE error occurs.
Testing Procedure:	Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\ Software\Microsoft\Internet Explorer\Main Determine the value data for the IEWatsonEnabled value. Criteria: The value data for the IEWatsonEnabled value must be 0
Test Nature:	Objective

Evidence:	
Finding:	

Part 3: Conduct the Audit Testing, Evidence and Findings

IE001 Internet Explorer Version

Evidence:	Workstation#1: The file version is 6.0.2800.1400 (Pass) Workstation #2: The file version is 6.0.2800.1400 (Pass)
Finding:	Passed.

IE002 Internet Explorer Internet Options Settings

Evidence:	Workstation#1: All Zones are configured as custom (Pass) Include all local (intranet) sites not listed in other zones – Selected (Fail) Include all sites that bypass the proxy server – Selected (Fail) Include all network paths (UNCs) – Selected (Fail) Privacy Settings – Medium (Pass) Advanced Options – See Table (Fail) Workstation #2: All Zones are configured as custom (Pass) Include all local (intranet) sites not listed in other zones – Selected (Fail) Include all sites that bypass the proxy server – Selected (Fail) Include all network paths (UNCs) – Selected (Fail) Privacy Settings – Medium (Pass) Advanced Options – See Table (Fail)
Finding:	Failed – Workstation #1 and Workstation #2.

PARAMETER	SETTING	Workstation #1	Workstation #2

Automatically check for Internet Explorer updates	Disable	Disable	Disable
Enable Install On Demand (Internet Explorer - [IE 6.0 only])	Disable	Disable	Disable
Enable Install On Demand (Other) [IE 6.0 only]	Disable	**Enabled**	**Enabled**
When searching	Do not search from the Address bar [or] Just display the results in the main window [or] [No option selected]	**Just go to most likely site**	**Just go to most likely site**
Check for signatures on downloaded programs [IE 6.0 only]	Enable	**Disabled**	**Disabled**
Use Private Communication Technology (PCT)1.0 [IE 5.5 only]	Disable	N/A	N/A
Use SSL 3.0	Enable	Enable	Enable
Use TLS 1.0	Enable	**Disabled**	**Disabled**
Warn about invalid site certificates	Enable	Enable	Enable
Warn if changing between secure and not secure mode	Enable	Enable	Enable
Warn if forms submittal is being redirected	Enable	Enable	Enable

IE003 Temporary Internet File Folder Access Control

Evidence:	Workstation#1: Do Not Save Encrypted Pages - Not Selected File Permissions Compliant – (Pass) Workstation #2: Do Not Save Encrypted Pages - Not Selected File Permissions Compliant – (Pass)
Finding:	Passed.

IE004 IE Advanced Internet Options Access Control

Evidence:	Workstation#1: Users can modify advanced options. (Fail) Workstation #2: Users can modify advanced options. (Fail)
Finding:	Failed – Workstation #1 and Workstation #2.

IE005 IE Security Zone Settings

Evidence: (Bold items indicate non compliant settings)

Parameter	**Workstation #1**			**Workstation #2**		
Zone	**Internet**	**Local Trusted**	**Restricted**	**Internet**	**Local Trusted**	**Restricted**
Download signed ActiveX controls	**Prompt**	Prompt	Disable	**Prompt**	Prompt	Disable
Download unsigned ActiveX controls	Disable	Disable	Disable	Disable	Disable	Disable
Initialize and script ActiveX controls not marked as safe	Disable	Disable	Disable	Disable	Disable	Disable

Run ActiveX controls and plug-ins	**Enable**	**Enable**	Disable	**Enable**	**Enable**	Disable
Script ActiveX controls marked safe for scripting	**Enable**	**Enable**	Disable	**Enable**	**Enable**	Disable
Allow cookies that are stored on your computer [IE 5.5 only]	N/A	N/A	N/A	N/A	N/A	N/A
Allow per-session cookies (not stored) [IE 5.5 only]	N/A	N/A	N/A	N/A	N/A	N/A
File download	Enable	Enable	Disable	Enable	Enable	Disable
Font download	**Enable**	Enable	**Prompt**	**Enable**	Enable	**Prompt**
Java permissions	N/A	N/A	N/A	N/A	N/A	N/A
Access data sources across domains	Disable	Prompt	Disable	Disable	Prompt	Disable
Allow META REFRESH [IE 6.0 only]	Enable	Enable	Disable	Enable	Enable	Disable
Display mixed content [IE 6.0 only]	Prompt	**Prompt**	Disable	Prompt	**Prompt**	Disable
Don't prompt for client certificate selection when no certificate or only one certificate exists	Disable	**Enable**	Disable	Disable	**Enable**	Disable
Drag and drop or copy and paste files	**Enable**	**Enable**	**Prompt**	**Enable**	**Enable**	**Prompt**
Installation of desktop items	**Prompt**	Prompt	Disable	**Prompt**	Prompt	Disable
Launching programs and files in an IFRAME	**Prompt**	Prompt	Disable	**Prompt**	Prompt	Disable
Navigate sub-frames across different domains	**Enable**	Enable	Disable	**Enable**	Enable	Disable
Software channel permissions	**Medium safety**	**Medium safety**	High safety	**Medium safety**	**Medium safety**	High safety
Submit non-encrypted form data	**Enable**	Enable	**Prompt**	**Enable**	Enable	**Prompt**
Userdata	**Enable**	Enable	Disable	**Enable**	Enable	Disable

persistence						
Active scripting	Enable	Enable	Disable	Enable	Enable	Disable
Allow paste operations via script	**Enable**	**Enable**	Disable	**Enable**	**Enable**	Disable
Scripting of Java applets	**Enable**	Enable	Disable	**Enable**	Enable	Disable
User Authentication – Logon	**Auto Logon on only Intranet Zones**	**Auto Logon on only Intranet Zones**	**Prompt for user name and password**	**Auto Logon on only Intranet Zones**	**Auto Logon on only Intranet Zones**	**Prompt for user name and password**

Finding:

Failed – Workstation #1 and Workstation #2.

IE006 IE Security Zone Settings Access Control

Evidence:	Workstation#1: Users can modify security options. (Fail) Workstation #2: Users can modify security options. (Fail)
Finding:	Failed – Workstation #1 and Workstation #2.

IE007 IE Ciphers

Evidence:	Workstation#1: DES 56/56 – Not Set (Fail) Triple DES 168/168 – Not Set (Fail) Workstation #2: DES 56/56 – Not Set (Fail) Triple DES 168/168 – Not Set (Fail)
Finding:	Failed – Workstation #1 and Workstation #2.

IE008 IE Hashes

Evidence:	Workstation#1: SHA Hash – Not Set (Fail) Workstation #2: SHA Hash – Not Set (Fail)
Finding:	Failed – Workstation #1 and Workstation #2.

IE0009 Root CA Certificate for IE

Evidence:	Workstation#1: Installed certificates comply with company policy. (Pass) Workstation #2: Installed certificates comply with company policy. (Pass)
Finding:	Passed.

IE010 IE Error Reporting Tool

Evidence:	Workstation#1: Key Not Present (Fail) Workstation #2: Key Not Present (Fail)
Finding:	Failed – Workstation #1 and Workstation #2.

Part 4: Audit Report

Executive summary

The audit of the JG Systems web browsers has been completed and the results are being presented in this report. I would like to mention that your staff was very cooperative in this effort and provided support as needed to the audit staff which helped make this effort successful.

The audit focused on the security of the organizations web browsers with the intent of identifying potential vulnerabilities and root causes of these issues. The goal was not only to identify the outstanding issues that need to be fixed, but to also make the system administrators aware of what needs to be done to eliminate the re-occurrence of these vulnerabilities.

As a general statement, the browsers appear to be set to many of the installation defaults. This is appropriate for some of the settings but for enhanced security additional precautions must be taken to protect the data and reputation of the organization. The system administration staff is utilizing the Windows Automatic Update service that is provided by Microsoft to keep the workstations up to date with the various patches that are required to eliminate vulnerabilities. Keeping your systems patched is a critical process in the security of the organization.

Audit Findings

The audit of the company's web browsers was conducted by manually reviewing the settings of two random workstations. The workstations were using Microsoft Windows XP as the Operating System and Internet Explorer version 6. The checklist that was used contained ten items that were reviewed. Following are the details of the audit findings:

IE001 Internet Explorer Version – Passed.

Un-patched versions of Internet Explorer have known significant security vulnerabilities. This includes privilege-elevation and information disclosure vulnerabilities. Without an effective patching process a significant vulnerability exists within the organization.

The browsers are currently configured with the latest patches. The workstations are configured with Windows Automatic Update which will keep the browsers at the current patch level.

IE002 Internet Explorer Internet Options Settings – Failed.

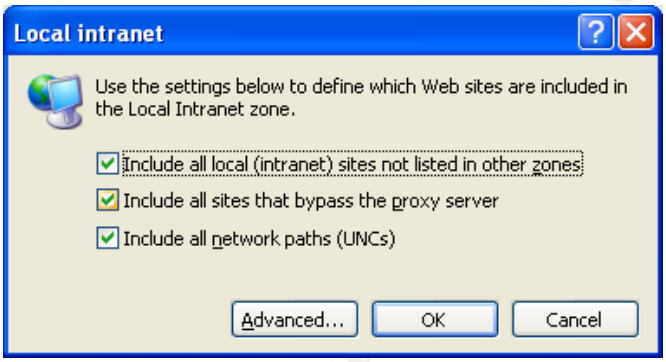
If the specified Internet Options are not configured as required, availability and information disclosure vulnerabilities can arise, malicious code could be introduced into

the client environment.

If options restricting the assignment of web sites to privileged IE Security Zones are not properly configured; malicious sites may be able to invoke programs intended for use only by trusted sites.

If options that enable stronger session protocols are disabled, information sent over SSL sessions may be more vulnerable to interception.

If options related to session encryption warnings are not enabled, a user may unintentionally send sensitive information over a non-encrypted session.



PARAMETER	SETTING	Workstation #1	Workstation #2
Automatically check for Internet Explorer updates	Disable	Disable	Disable
Enable Install On Demand (Internet Explorer - [IE 6.0 only])	Disable	Disable	Disable
Enable Install On Demand (Other) [IE 6.0 only]	Disable	**Enabled**	**Enabled**
When searching	Do not search from the Address bar [or] Just display the results in the main window [or] [No option	**Just go to most likely site**	**Just go to most likely site**

	selected]		
Check for signatures on downloaded programs [IE 6.0 only]	Enable	**Disabled**	**Disabled**
Use Private Communication Technology (PCT)1.0 [IE 5.5 only]	Disable	N/A	N/A
Use SSL 3.0	Enable	Enable	Enable
Use TLS 1.0	Enable	**Disabled**	**Disabled**
Warn about invalid site certificates	Enable	Enable	Enable
Warn if changing between secure and not secure mode	Enable	Enable	Enable
Warn if forms submittal is being redirected	Enable	Enable	Enable

IE003 Temporary Internet File Folder Access Control – Passed.

If web pages displayed during an encrypted (SSL) session are cached in users Temporary Internet files folder and access to that folder is not properly restricted, an information disclosure vulnerability exists. Third parties with access to a users Temporary Internet files folder may be able to recover sensitive data sent during an encrypted browser session.

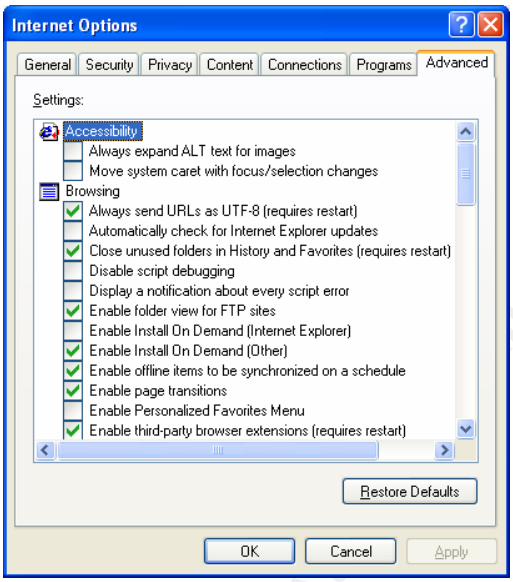
The browsers are not configured to disable the caching of the encrypted pages but the files associated with the Temporary Internet File folder meet the designated access controls which eliminate the vulnerability.

IE004 IE Advanced Internet Options Access Control – Failed.

If users are able to change the Internet Options Advanced settings, availability and information disclosure vulnerabilities can arise. Information disclosures may occur as the result of weakened security settings that no longer restrict data access. Client

availability and data integrity issues can result from settings that allow malicious code to execute.

Workstations have not been restricted to prevent users from making modifications to the advanced options of the web browser. This ability provides the user with the ability to circumvent security settings without the knowledge of the SA staff.



IE005 IE Security Zone Settings – Failed.

If the specified Security Zones settings are not configured as required, availability and information disclosure vulnerabilities can arise.

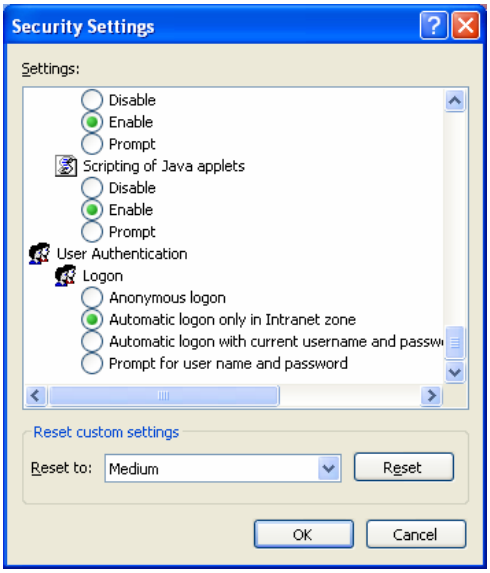
If options restricting the execution of ActiveX controls are not properly configured, malicious code could be executed in the client environment.

If options restricting downloads and other types of data flow are not properly configured, malicious code could be introduced into the client environment and client data could be disclosed.

If options restricting the execution of Java applets are not properly configured, malicious code could be executed in the client environment.

If options related to session encryption warnings are not enabled, a user may unintentionally send sensitive information over a non-encrypted session.

Many of the settings are not configured in accordance with security policy.



Parameter	Workstation #1			Workstation #2		
Zone	**Internet**	**Local Trusted**	**Restricted**	**Internet**	**Local Trusted**	**Restricted**
Download signed ActiveX controls	**Prompt**	Prompt	Disable	**Prompt**	Prompt	Disable
Download unsigned ActiveX controls	Disable	Disable	Disable	Disable	Disable	Disable
Initialize and script ActiveX controls not marked as safe	Disable	Disable	Disable	Disable	Disable	Disable
Run ActiveX controls and plug-ins	**Enable**	**Enable**	Disable	**Enable**	**Enable**	Disable
Script ActiveX controls marked safe for scripting	**Enable**	**Enable**	Disable	**Enable**	**Enable**	Disable
Allow cookies that are stored on your computer [IE 5.5 only]	N/A	N/A	N/A	N/A	N/A	N/A
Allow per-session cookies (not stored) [IE 5.5 only]	N/A	N/A	N/A	N/A	N/A	N/A
File download	Enable	Enable	Disable	Enable	Enable	Disable
Font download	**Enable**	Enable	**Prompt**	**Enable**	Enable	**Prompt**
Java permissions	N/A	N/A	N/A	N/A	N/A	N/A
Access data sources across domains	Disable	Prompt	Disable	Disable	Prompt	Disable
Allow	Enable	Enable	Disable	Enable	Enable	Disable

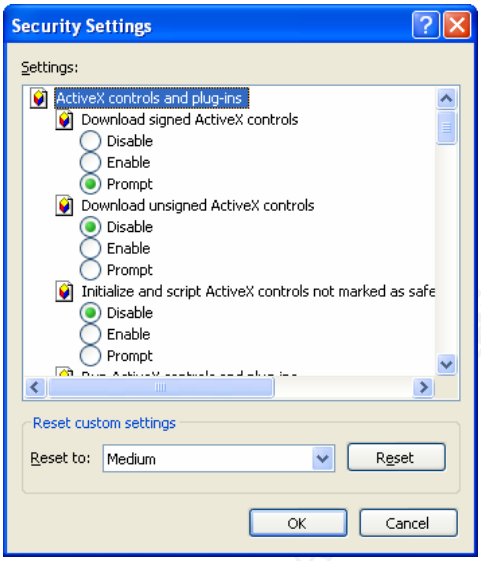
META REFRESH [IE 6.0 only]						
Display mixed content [IE 6.0 only]	Prompt	**Prompt**	Disable	Prompt	**Prompt**	Disable
Don't prompt for client certificate selection when no certificate or only one certificate exists	Disable	**Enable**	Disable	Disable	**Enable**	Disable
Drag and drop or copy and paste files	**Enable**	**Enable**	**Prompt**	**Enable**	**Enable**	**Prompt**
Installation of desktop items	**Prompt**	Prompt	Disable	**Prompt**	Prompt	Disable
Launching programs and files in an IFRAME	**Prompt**	Prompt	Disable	**Prompt**	Prompt	Disable
Navigate sub-frames across different domains	**Enable**	Enable	Disable	**Enable**	Enable	Disable
Software channel permissions	**Medium safety**	**Medium safety**	High safety	**Medium safety**	**Medium safety**	High safety
Submit non-encrypted form data	**Enable**	Enable	**Prompt**	**Enable**	Enable	**Prompt**
Userdata persistence	**Enable**	Enable	Disable	**Enable**	Enable	Disable
Active scripting	Enable	Enable	Disable	Enable	Enable	Disable
Allow paste operations via script	**Enable**	**Enable**	Disable	**Enable**	**Enable**	Disable
Scripting of Java applets	**Enable**	Enable	Disable	**Enable**	Enable	Disable
User Authentication – Logon	**Auto Logon on only Intranet Zones**	**Auto Logon on only Intranet Zones**	**Prompt for user name and password**	**Auto Logon on only Intranet Zones**	**Auto Logon on only Intranet Zones**	**Prompt for user name and password**

IE006 IE Security Zone Settings Access Control – Failed.

If users are able to change the Internet Options Security Zone settings, availability and information disclosure vulnerabilities can arise. Information disclosures may occur as the result of weakened security settings that no longer restrict data access. Client

availability and data integrity issues can result from settings that allow malicious code to execute.

Workstations have not been restricted to prevent users from making modifications to the security settings of the web browser. This ability provides the user with the ability to circumvent security settings without the knowledge of the SA staff.



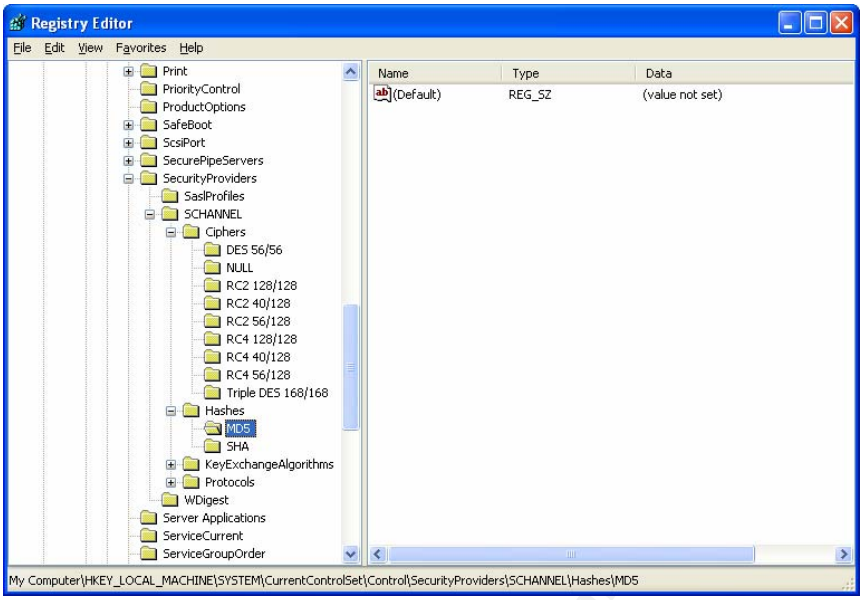
IE007 IE Ciphers – Failed.

If the specified SSL cipher options are not configured as required, information disclosure vulnerabilities can arise. The use of null or weaker encryption algorithms could allow intercepted session data to be more easily decrypted.

The SSL ciphers are not configured to utilized DES and Triple DES encryption.

IE008 IE Hashes – Failed.

If the specified SSL hash options are not configured as required, information integrity vulnerabilities can arise. The use of weaker hash algorithms could allow intercepted session data to be more easily modified without detection.



IE0009 Root CA Certificate for IE – Passed.

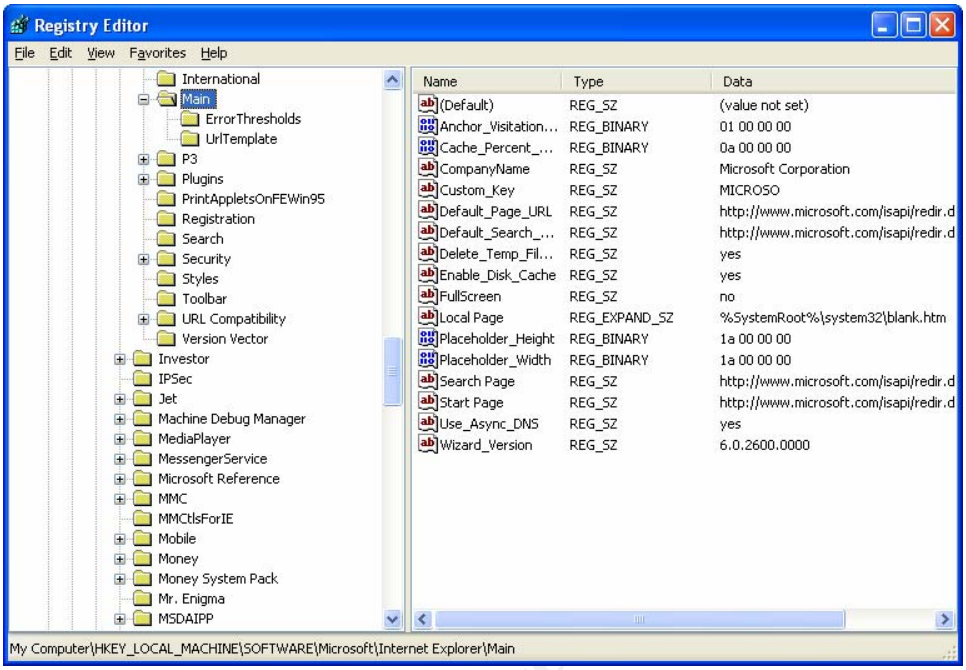
If non approved Root Certificate Authority certificates are installed, information disclosure vulnerabilities can result. Web browser sessions may be established with sites impersonating the web site for which a connection was intended.

If an unapproved Root Certificate Authority certificate is installed, users may invalidly authenticate a web sites identity and unintentionally allow a session with a counterfeit site.

IE010 IE Error Reporting Tool – Failed.

If the Error Reporting tool for IE is enabled, an information disclosure vulnerability exists. A user may send sensitive information in a document to Microsoft when an IE error occurs.

The IE error reporting tools is not configured on the workstations.



Audit Recommendations

To eliminate findings in the future and mitigate the potential security risks associated with accessing the world wide web, the company needs to the following steps:

- Hire an auditor to perform a security review of the Operating System software that is installed on the workstations.
- Continue the use of Windows Automatic Update to address patches for Internet Explorer and the Operating System software.
- Establish an automated process for maintaining the configuration of the browsers. Microsoft has a tool called the IE Zero Administration Kit (IEAK) that the SAs can use to automate the maintenance of the web browser and eliminate much of the manual work that needs to be performed.
- Make the necessary changes that have been identified in this audit to bring the web browser software into compliance.

Costs.

Many of the problems that have been identified in this audit require only the time of the systems administrators to correct. This is a relatively lost cost in comparison to the costs associated with loss of data or a damaged reputation. To make this process easier on the SA staff, the automated tools that have been identified are available free of charge from the vendor.

Reference List:

The SANS Institute Conference Track 7 (2004, April). *Auditing Networks, Perimeters, and Systems.* Course materials presented at the 2004 SANS Institute conference, Orlando, Fl.

The Central Arizona College settings for Internet Explorer 6.0.
http://www.centralaz.edu/inetclasses/setup/IE-Complete-Settings.htm

The University of Maryland University College web browser settings.
http://www.umuc.edu/library/database/browser.html

Penn Computing securing of the desktop environment.
http://www.upenn.edu/computing/security/checklists/desktop.html

Microsoft Corporation. TechNet – Internet Explorer Checklist.
http://www.microsoft.com/technet/security/chklist/iecl.mspx

Microsoft Corporation. Checklist for preparing to use the IEAK.
http://www.microsoft.com/resources/documentation/ie/6/all/reskit/en-us/part7/z04ie6rk.mspx

The National Security Agency. Guide to Securing Windows NT/9x Clients in a Windows 2000 Network. 6 March 2002.

Defense Information Systems Agency. Desktop Application STIG, Version 2 Release 0. 26 July 2004.

Last Updated: May 23rd, 2017

Upcoming Training

SANS Secure Europe 2017	**Amsterdam, Netherlands**	**Jun 12, 2017 - Jun 20, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**