the CENTER for INTERNET SECURITY

Security Configuration Benchmark For

Mozilla Firefox 3.5

Version 1.0.0

January 7th, 2010

http://cisecurity.org
feedback@cisecurity.org

Terms of Use Agreement

Background.

CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No representations, warranties and covenants.

CIS makes no representations, warranties or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness or completeness of any Product or Recommendation. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties or covenants of any kind.

User agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**we**") agree and acknowledge that:

No network, system, device, hardware, software or component can be made fully secure;
We are using the Products and the Recommendations solely at our own risk;

We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;

We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at it sole option to do so; and

Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of limited rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of intellectual property rights; limitations on distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights." Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special rules.

CIS has created and will from time to time create special rules for its members and for other

persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules. CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of law; jurisdiction; venue.

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions. We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

Table of Contents

1. Overview

This document, *Security Configuration Benchmark for Web Browsers*, provides prescriptive guidance for establishing a secure configuration posture for Firefox 3.5.6 running on *Microsoft Windows Version 5.1 XP Professional: Service Pack 3 and Windows Vista (x86)*. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

1.1 Consensus Guidance

This guide was created using a consensus review process comprised of volunteer and contract subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the CIS benchmark. If you are interested in participating in the consensus review process, please send us a note to feedback@cisecurity.org.

1.2 Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel, who plan to develop, deploy, assess, or secure solutions that incorporate Mozilla Firefox 3.5.

1.3 Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Authors
Waqas Nazir, *Digital Security, LLC.*

Contributors and Reviews
Ron Colvin, *National Aeronautics and Space Administration*
Blake Frantz, *Center for Internet Security*
Patrick McCafferty, *VMC, Inc.*
Steven Piliero, *Center for Internet Security*
Andy Sampson, *National Security Agency*
David Skrdla, *University of Oklahoma*

1.4 Typographic Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

1.5 Configuration Levels

This section defines the configuration levels that are associated with each benchmark recommendation. Configuration levels represent increasing levels of security assurance.

1.5.1 Level-I Benchmark Settings/Actions

Level-I Benchmark recommendations are intended to:

- be practical and prudent;
- provide a clear security benefit;
- not negatively inhibit the utility of the technology beyond acceptable means

1.5.2 Level-II Benchmark Settings/Actions

Level-II Benchmark recommendations exhibit one or more of the following characteristics:

- may negatively inhibit the utility or performance of the technology
- act as a defense in depth measure

1.6 Scoring Status

This section defines the scoring statuses used within this document. The scoring status indicates whether compliance with the given recommendation is discernable in an automated manner.

1.6.1 Scorable

The platform's compliance with the given recommendation can be determined via automated means.

1.6.2 Not Scorable

The platform's compliance with the given recommendation cannot be determined via automated means.

2. Recommendations

2.1 Network Connections:

This section will discuss how to securely configure network connections in Firefox.

2.1.1 Validate Proxy Settings (Level I, Not Scorable)

Description:
Firefox can be configured to use one or more proxy servers. When a proxy server is configured for a given protocol (HTTP, FTP, Gopher, etc), Firefox will send applicable requests to that proxy server for fulfillment. If is recommended that the list of proxy servers configured in Firefox be reviewed to ensure it contains only trusted proxy servers.

Rationale:
Depending on the protocol used, the proxy server will have access to read and/or alter all information communicated between Firefox and the target server, such a web site.

Remediation:
Perform the following procedure:

1. Click on 'Tools'
2. Select 'Options' from the drop down.
3. Click on 'Advanced' Button on Options window
4. Click on 'Network' Tab
5. Click on 'Settings' Button
6. Ensure that the proxy listed (if any) is the one configured and approved by the enterprise.

Audit:
Perform the following procedure:

1. Click on 'Tools'
2. Select 'Options' from the drop down.
3. Click on 'Advanced' Button on Options window
4. Click on 'Network' Tab
5. Click on 'Settings' Button
6. Ensure that the proxy listed (if any) is the one configured and approved by the enterprise.

2.2 Updating Firefox

This section will discuss how to enable auto updates in Firefox.

2.2.1 Enable Auto Update (Level I, Scorable)

Description:
This configuration will show how to enable updates for Firefox and extensions installed on Firefox.

Rationale:
Security updates are critical in ensuring that a user a safe is from known vulnerabilities. Therefore, automatic checking of updates should be enabled.

Remediation:
Perform the following procedure:

1. Click on 'Tools'
2. Click on 'Options'
3. Click on 'Advanced' Icon
4. Click on 'Update' Tab
5. Select 'Firefox,' 'Installed Add-ons,' and 'Search Engines' under the 'Automatically check for updates to:' section.
6. Select 'Automatically download and install the update' option in the 'When updates to Firefox are found' section
7. Select the 'Warn me if this will disable any of Add-ons' sub-option.
8. Click 'OK'

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "app.update.auto"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

If no results are returned it means that auto update has been enabled for the current profile. Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

Note: This setting is not required where organizations are automatically managing the update process remotely.

2.2.2 Enable Update Notifications (Level I, Scorable)

Description:
This configuration will ensure that a user is notified when an update is available.

Rationale:
This will help users to keep Firefox up-to-date.

Remediation:

Perform the following procedure:

1. Type 'about:config' in the address bar
2. Type 'Security' in the filter
3. Set the preference listed with the values specified below

```
security.xpconnect.plugin.unrestricted=true
```

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "security.xpconnect.plugin.unrestricted"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

This will not return any results if Firefox is configured correctly for the current profile.
Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.3 Encryption Settings

This section will discuss how to set up encryption settings in Firefox.

2.3.1 Enable SSL 3.0 and TLS 1.0 (Level I, Scorable)

Description:
This configuration will show how to enable SSL 3.0 and TLS 1.0 for Firefox.

Rationale:
Enabling these protocols will allow Firefox to enforce selection of higher SSL and TLS encryption key lengths and more robust protocols

Remediation:
Perform the following procedure:

1. Click on 'Tools'
2. Click on 'Options'
3. Click on 'Advanced' Icon
4. Click on 'Encryption' Tab
5. Select Use SSL 3.0, Use TLS 1.0 under 'Protocols' section
6. Select 'Ask me everytime' under Certificates.
7. Click 'OK'

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "security.enable_ssl3"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

If no results are returned it means that auto update has been enabled for the current user.
Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.3.2 Enable Warning of Loading Mixed Content (Level I, Scorable)

Description:
This will warn users when unencrypted data is loaded in an SSL encrypted session.

Rationale:
Enabling this setting will alert a user when some content on a secure communication channel is coming under a non secure channel. For example an SSL website can request part of content on a page under a non-SSL session. This can leave users vulnerable to eavesdropping and Man in the Middle attacks.

Remediation:
Use the following procedure:

1. Click on 'Tools'
2. Click on 'Options'
3. Click on 'Security' Icon
4. Click on 'Settings' Button under the 'Warnings' section
5. Select 'I'm about to view an encrypted page that contains some unencrypted information.'
6. Click 'OK'

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "security.warn_viewing_mixed"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

If no results are returned it means that auto update has been enabled for the current profile. Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.3.3 Enable Warning of Using Weak Encryption (Level I, Scorable)

Description:
This will warn users when a website is using weaker encryption.

Rationale:
This will protect users from the compromise of their data due to weak encryption.

Remediation:
Use the following procedure:

1. Click on 'Tools'
2. Click on 'Options'
3. Click on 'Security' Icon
4. Click on 'Settings' Button under the 'Warnings' section

5. Select 'I am about to view a page that uses low-grade encryption.'
6. Click 'OK'

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "security.warn_entering_weak"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

If no results are returned it means that auto update has been enabled for the current profile. Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.3.4 Enable Online Certificate Status Protocol (Level I, Scorable)

Description:
Firefox checks with Online Certification Status Protocol (OCSP) to ensure that the certificates are valid. Firefox can validate a certificate if an OCSP server is specified by the certificate or an OCSP server can be configured manually.

Rationale:
To provide assurance on the validity of encryption Certificates these option should be enabled.

Remediation:
Perform the following procedure:

1. Click on 'Tools'
2. Click on 'Options'
3. Click on 'Advanced' Icon
4. Click on 'Encryption' Tab
5. Click on 'Validation' Button in the Certificates section
6. Select 'Use the Online Certificate Status Protocol (OCSP) to confirm the current validity of certificates' option
7. Click 'OK'
8. Click 'OK'

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "security.OCSP.enabled"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

If no results are returned it means that auto update has been enabled for the current profile. Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.4 Add-Ons Settings

This section will discuss how to set up Add Ons in Firefox. Some Add-ons such as NoScript and Flashblock can be installed to provide additional protection to the end user. [1]

2.4.1 Disabling Auto-Install of Add-Ons (Level I, Scorable)

Description:
This configuration will show how to ensure that no website is allowed to automatically install AddOns. Also, it will list how to ensure that proper notifications are shown when installing Add-Ons.

Rationale:
Add-Ons are extensions of the browser that add new functionality to Firefox or change its appearance. These run in a user's session allowing them do manipulate data and the behavior of the way Firefox interacts with other application and user commands. If malicious Add-Ons are installed automatically, a user's security could be completely compromised.

Remediation:
Use the following procedure:

1. Click on 'Tools'
2. Click on 'Options'
3. Click on 'Security' Icon
4. Select 'Warn me when sites try to install add-ons' under the Top section of the dialog
5. Next, click on 'Exceptions' Button and then Click on 'Remove All Sites'
6. Hit 'Close'
7. Click 'OK'

Audit:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "xpinstall.whitelist.required"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

If no results are returned it means that auto update has been enabled for the current profile. Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.4.2 Secure Application Plug-ins (Level I, Not Scorable)

Description:

Some active content such as audio and video can be automatically loaded by Firefox on websites.

Rationale:
Some malicious websites can have active content to exploit vulnerabilities in active content handling application plug-in. It is recommended as a defense-in-depth to always prompt when a website is about to load active content which is not trusted.

Remediation:
Perform the following procedure:

1. In Firefox Browser
2. Click on 'Tools'
3. Click on 'Options'
4. Click on 'Application' Icon
5. Select all Content Types listed which are not trusted, and in the Action select 'Always ask' in the drop down
6. Hit 'OK'

Audit:
Perform the following procedure:

1. In Firefox Browser
2. Click on 'Tools'
3. Click on 'Options'
4. Click on 'Application' Icon
5. Check that all Content Types listed, which are not trusted, and in the Action verify that 'Always ask' is selected in the drop down
6. Hit 'OK'

2.5 Dynamic Content Settings

Dynamic content consists of scripts and native browser objects which can change the content of a browser window without the knowledge of a user. This section will show how to lock down dynamic content in Firefox.

2.5.1 Disable Closing of Windows via Scripts (Level II, Scorable)

Description:
Firefox can be configured to prevent script from closing browser windows. It is recommended that script be prevented from closing browser windows.

Rationale:
Preventing an arbitrary web site from closing the browser window will reduce the probability of a user losing work or state being performed in another tab within the same window.

Remediation:

Perform the following procedure:

1. Type ‘about:config’ in the address bar
2. Type ‘dom’ in the filter
3. Set the preference listed with the values specified below

```
dom.allow_scripts_to_close_windows=false
```

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "dom.allow_scripts_to_close_windows"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

This will not return anything if Firefox is configured correctly for the current profile.
Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.5.2 Disable Caching of SSL Pages (Level I, Scorable)

Description:
Firefox can locally cache the content of SSL pages on disk. It is recommended that caching SSL content be disabled.

Rationale:
This will protect users confidential information from unauthorized disclosure.

Remediation:
Perform the following procedure:

1. Type ‘about:config’ in the address bar
2. Type ‘browser’ in the filter
3. Set the preference listed with the values specified below

```
browser.cache.disk_cache_ssl=false
```

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "browser.cache.disk_cache_ssl"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

This will not return anything if Firefox is configured correctly for the current profile.
Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.5.3 Disable Downloading on Desktop (Level I, Scorable)

Description:
Firefox can download content on the desktop or other locations. It is recommended not to download files on desktop.

Rationale:
This will protect from downloading content on desktop and tricking users into running malicious binaries.

Remediation:
Perform the following procedure:

1. Type 'about:config' in the address bar
2. Type 'browser' in the filter
3. Set the preference listed with the values specified below

```
browser.download.folderList=2
```

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "browser.download.folderList"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

This will return the following if Firefox is configured correctly for the current profile.

```
prefs.js:user_pref("browser.download.folderList", 2);
```

Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.5.4 Enable Alerting before Running Executable from Download Manager (Level I, Scorable)

Description:
Firefox can be configured to alert the user before running executables from the Download Manager. It is recommended that this capability be enabled.

Rationale:
Alerting the user before running executables from the Download Manager will ensure the user does not accidently run potentially malicious content.

Remediation:
Perform the following procedure:

1. Type 'about:config' in the address bar
2. Type 'browser' in the filter

3. Set the preference listed with the values specified below

```
browser.download.manager.alertOnEXEOpen=true
```

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "browser.download.manager.alertOnEXEOpen"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

   This will return the following if Firefox is configured correctly for the current profile.

```
prefs.js:user_pref("browser.download.manager.alertOnEXEOpen", true);
```

Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.5.5 Enable Virus Scanning for Downloads (Level I, Scorable)

Description:
Firefox can be configured to scan downloads for viruses. It is recommended that this capability be enabled.

Rationale:
This will ensure that a downloaded file is scanned for viruses before the user has an opportunity to interact with the download.

Remediation:
Perform the following procedure:

1. Type 'about:config' in the address bar
2. Type 'browser' in the filter
3. Set the preference listed with the values specified below

```
browser.download.manager.scanWhenDone=true
```

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "browser.download.manager.scanWhenDone"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

   This will not return anything if Firefox is configured correctly for the current user.

Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.5.6 Block Reported Web Forgeries (Level I, Scorable)

Description:
Firefox can be configured to alert the user that the site they are visiting is malicious. It is recommended that this capability be enabled.

Rationale:
Enabling this feature will decrease the probability of a user falling victim to a phishing attack or unknowingly disclosing sensitive information to an untrusted party.

Remediation:
Perform the following procedure:

1. Type 'about:config' in the address bar
2. Type 'browser' in the filter
3. Set the preference listed with the values specified below

```
browser.safebrowsing.enabled=true
```

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "browser.safebrowsing.enabled"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

   This will not return anything if Firefox is configured correctly for the current user.

Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.5.7 Block Reported Attack Sites (Level I, Scorable)

Description:
Firefox can be configured to alert the user that the site they are visiting is malicious. It is recommended that this capability be enabled.

Rationale:
Enabling this feature will decrease the probability of a user's browser or system being exploited by known malware.

Remediation:
Perform the following procedure:

1. Type 'about:config' in the address bar
2. Type 'browser' in the filter

3. Set the preference listed with the values specified below

```
browser.safebrowsing.malware.enabled=true
```

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "browser.safebrowsing.malware.enabled"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

This will not return anything if Firefox is configured correctly for the current user.

Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.5.8 Disable Displaying Javascript in History URLs (Level I, Scorable)

Description:
This will ensure that JavaScript URLs are not displayed in the history bar.

Rationale:
Various browser elements, even a simple link, can embed javascript: URLs and access the javascript: protocol. The JavaScript statement used in a javascript: URL can be used to encapsulate a specially crafted URL that performs a malicious function.

Remediation:
Perform the following procedure:

1. Type 'about:config' in the address bar
2. Type 'browser' in the filter
3. Set the preference listed with the values specified below

```
browser.urlbar.filter.javascript=true
```

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "browser.urlbar.filter.javascript"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

This will not return anything if Firefox is configured correctly.

2.6 Network Settings

This section provides guidance for configuring portions of Firefox exposed via the Network Settings dialog.

2.6.1 Enable SSPI Authentication (Level I, Scorable)

Description:
Firefox can be configured to leverage the Microsoft Windows Security Support Provider Interface (SSPI). It is recommended that this capability be enabled.

Rationale:
This will protect users from using weaker authentication.

Remediation:
Perform the following procedure:

1. Type 'about:config' in the address bar
2. Type 'network.auth' in the filter
3. Set the preference listed with the values specified below

```
network.auth.use-sspi=true
```

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "network.auth.use-sspi"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

This will not return anything if Firefox is configured correctly for the current profile. Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.6.2 Disable Referer from an SSL Website (Level I, Scorable)

Description:
Firefox can be configured to omit the HTTP `Referer` header when the referring site is protected by SSL. An HTTP `Referer` header provides the referred site with the URL of the referring site.

Rationale:
It is possible that the URL of the SSL-protected, referring site contains sensitive information. By preventing Firefox from sending this URL, via an HTTP `Referer` header, to sites referred to by the SSL protected site an avenue for information disclose is eliminated.

Remediation:
Perform the following procedure:

1. Type 'about:config' in the address bar
2. Type 'network' in the filter
3. Set the preference listed with the values specified below

```
network.http.sendSecureXSiteReferrer=false
```

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "network.http.sendSecureXSiteReferrer"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

   This will return the following result if Firefox is configured correctly for the current profile.

```
prefs.js:user_pref("network.http.sendSecureXSiteReferrer", false);
```

Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.6.3 Disable Sending LM Hash (Level I, Scorable)

Description:
Firefox can be configured to send an LM Hash when authenticating to resources that request this authentication type. It is recommended that this capability be disabled.

Rationale:
The LM Hashing algorithm contains weaknesses that can be exploited to derive plain text authentication credentials.

Remediation:
Perform the following procedure:

1. Type 'about:config' in the address bar
2. Type 'network.ntlm' in the filter
3. Set the preference listed with the values specified below

```
network.ntlm.send-lm-response=false
```

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "network.ntlm.send-lm-response"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

   This will not return any results if Firefox is configured correctly for the current profile.

Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.7 Privacy Settings

A user's browser can provide information such as browsing history to Internet resources which can result in the compromise of the privacy of a user. This section will outline how to enable the controls to guard user privacy.

2.7.1 Accept Only 1st Party Cookies (Level I, Scorable)

Description:
Cookies are used to track valid session on internet websites. Securing cookie handling will help secure a user's browser session.

Rationale:
These cookies are typically used to uniquely identify a user's session on a website. However, these cookies can be used by third party sites and malicious sites to track a user's activity on the web. Also, they can be used to store sensitive personally identifiable information. Cookie settings should be configured such that malicious websites cannot set the cookies.

Remediation:
Perform the following procedure:

1. In Firefox Browser
2. Click on 'Tools'
3. Click on 'Options'
4. Click on 'Privacy' Icon
5. Check 'Accept Cookies from Sites'
6. Ensure that 'Accept third-party cookies' is Unchecked
7. Hit 'OK'

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following commands:

```
findstr /isl /a:6 "network.cookie.cookieBehavior"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

This will return the following results if Firefox is configured correctly.

```
user_pref("network.cookie.cookieBehavior", 1);
```

Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.7.2 Disallow Credential Storage (Level I, Scorable)

Description:
Firefox allows credentials to be stored for certain websites.

Rationale:
Credentials can be compromised if the computer is shared with other users. This setting will ensure that the passwords are not stored for websites.

Remediation:
Perform the following procedure:

1. In Firefox Browser
2. Click on 'Tools'
3. Click on 'Options'
4. Click on 'Security' Icon
5. Unselect 'Remember passwords for sites'
6. Click 'Saved Password'
7. If there are any saved passwords listed in the dialog, click on 'Remove All'
8. Click 'OK'

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following commands:

```
findstr /isl /a:6 "signon.rememberSignons"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

This will return the following result:

```
user_pref("signon.rememberSignons", false);
```

`false` indicates that any passwords previously saved will be deleted when the saved data is cleared for the current profile. Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.7.3 Disable Prompting for Credential Storage (Level II, Scorable)

Description:
Firefox can prompt when credentials are entered in website forms.

Rationale:
This setting will ensure that Firefox does not prompt for storing passwords which will be stored by Firefox. Stored credentials/sensitive data pose a risk as they can be compromised by malicious websites using information leakage bugs/advisories in Firefox.

Remediation:
Perform the following procedure:

1. Type 'about:config' in the address bar
2. Type 'security' in the filter
3. Set the preference listed with the values specified below

```
security.ask_for_password=0
```

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following commands:

```
findstr /isl /a:6 "security.ask_for_password"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

This will result in no output if the password setting is set appropriately for the current profile. Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

Note: This option should be considered Level I for shared computing resources.

2.7.4 Delete History and Form Data (Level II, Scorable)

Description:
Firefox can store the sites visited, information typed in forms, and downloads from Internet resources.

Rationale:
The History, form data, download information can be compromised due to information leakage bugs in Firefox.

Remediation:
Perform the following procedure:

1. In Firefox Browser
2. Click on 'Tools'
3. Click on 'Options'
4. Click on 'Privacy' Icon
5. Select 'Use custom settings for History' from the 'Firefox will:' section
6. Uncheck 'Remember my browsing history for at least' checkbox
7. Hit 'OK'

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following commands:

```
findstr /isl /a:6 "browser.history_expire_days"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

This will return:

```
user_pref("browser.history_expire_days", 0);
```

The zero (0) is indication that no history is being saved for the current profile. Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

Note: This option should be considered Level I for shared computing resources.

References:
1. CVE-2009-3370

2.7.5 Delete Download History (Level II, Scorable)

Description:
Firefox can store downloads from Internet resources.

Rationale:
The download history can be compromised due to information leakage bugs/advisories in Firefox.

Remediation:
Perform the following procedure:

1. In Firefox Browser
2. Click on 'Tools'
3. Click on 'Options'
4. Click on 'Privacy' Icon
5. Uncheck 'Remember download history'
6. Hit 'OK'

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "browser.download.manager.retention"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*
```

This will return:

```
user_pref("browser.download.manager.retention", 0);
```

Zero (0) is an indication that no download history is retained for the current profile. Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

References:

1. CVE-2009-3370

Note: This option should be considered Level I for shared computing resources.

2.7.6 Delete Search and Form History (Level II, Scorable)

Description:
Firefox can store Search and Form Data from Internet resources.

Rationale:
The Search and Form Data can be compromised due to information leakage bugs in Firefox.

Remediation:
Perform the following procedure:

1. In Firefox Browser
2. Click on 'Tools'
3. Click on 'Options'
4. Click on 'Privacy' Icon
5. Uncheck 'Remember search and form history' checkbox
6. Hit 'OK'

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "browser.formfill.enable"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*
```

This will return:

```
user_pref("browser.formfill.enable ", false);
```

Zero (0) is an indication that no download history is retained for the current profile. Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

References:

1. CVE-2009-3370

Note: This option should be considered Level I for shared computing resources.

2.7.7 Block Pop-up Windows (Level I, Scorable)

Description:
The Pop-up Blocker is used to block Pop-ups which a website might open with or without any user interaction. These Pop-Ups can be used to open un-trusted malicious content.

Rationale:
By enabling the Pop-up blocker all Pop-ups will be blocked which will guard a user against any attacks launched using a Pop-up.

Remediation:
Perform the following procedure:

1. In Firefox Browser
2. Click on 'Tools'
3. Click on 'Options'
4. Click on 'Content' Icon
5. Select 'Block pop-up windows'
6. Click on 'Exceptions …'
7. Click on 'Remove all Sites …'
8. Click 'Close'
9. Hit 'OK

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "privacy.popups.policy"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

This will result in no output if the browser is configured as recommended for the current profile. Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.7.8 Clear SSL Form Session Data (Level II, Scorable)

Description:
This will ensure that the form data stored in an SSL Secure session is cleared when the session ends.

Rationale:
The form data stored during a SSL session can be compromised due to information leakage bugs affecting Firefox.

Remediation:

Perform the following procedure:

1. Type ‘about:config’ in the address bar
2. Type ‘privacy’ in the filter
3. Set the preference listed with the values specified below

```
browser.sessionstore.privacy_level=1
```

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "browser.sessionstore.privacy_level"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

This will not return anything if Firefox is configured correctly for the current profile.
Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

Note: This option should be considered Level I for shared computing resources.

References:
1. CVE-2009-3370

2.7.9 Enable Warning When Entering Insecure Site (Level I, Scorable)

Description:
Firefox can notify users when a user enters an insecure (non-SSL) site from an encrypted SSL site.

Rationale:
The recommended state will ensure the user is aware that the confidentiality of the information they are sending in the given Firefox tab or window is no longer protected.

Remediation:
Perform the following procedure:

1. Type ‘about:config’ in the address bar
2. Type ‘Security’ in the filter
3. Set the preference listed with the values specified below

```
security.warn_entering_weak=true
```

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "security.warn_entering_weak"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

This will not return any results if Firefox is configured correctly for the current profile. Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.7.10 Enable Warning When Submitting Clear Text Form Data (Level I, Scorable)

Description:
Firefox can notify users when a user sends form data to an insecure (non-SSL) site.

Rationale:
This will protect users from sending clear text data to website which can be sensitive in nature.

Remediation:
Perform the following procedure:

1. Type 'about:config' in the address bar
2. Type 'Security' in the filter
3. Set the preference listed with the values specified below

```
security.warn_submit_insecure=true
```

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "security.warn_submit_insecure"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

This will not return any results if Firefox is configured correctly for the current profile. Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.8 Advanced JavaScript Settings:

This section will provide guidance on how to use advanced JavaScript settings to guard against certain attacks.

2.8.1 Disable JavaScript's Ability to Hide the Status Bar (Level I, Scorable)

Description:

Status Bar shows the location of the content when a user visits a link or when content is being downloaded on a web page.

Rationale:
Some malicious websites can use JavaScript to hide the status bar so that a user cannot determine the location of the content for hyperlinks and downloads. It is recommended to disallow JavaScript from hiding the Status Bar.

Remediation:
Perform the following procedure:

1. In Firefox Browser
2. Click on 'Tools'
3. Click on 'Options'
4. Click on 'Content' Icon
5. Click on 'Advanced' button next to 'Enable JavaScript'
6. Unselect 'Hide Status bar' checkbox
7. Hit 'OK'

Audit:
Perform **the following** procedure**:**

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "dom.disable_window_open_feature.status"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

This will not return anything if Firefox is configured correctly for the current profile.
Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.8.2 Disable JavaScript's Ability to Change the Status Bar Text (Level I, Scorable)

Description:
Status Bar shows the location of the content when a user hovers of a hyperlink, a user visits a link, or when content is being downloaded on a web page.

Rationale:
Some malicious websites can use JavaScript to manipulate the text on the status bar so that a user cannot determine the actual location of the content for hyperlinks and downloads. It is recommended to disallow JavaScript from changing the text on the Status Bar.

Remediation:
Perform the following procedure:

1. In Firefox Browser

2. Click on 'Tools'
3. Click on 'Options'
4. Click on 'Content' Icon
5. Click on 'Advanced' button next to 'Enable JavaScript'
6. Unselect 'Change Status bar text' checkbox
7. Click 'OK'

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 " dom.disable_window_status_change"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

This will not return anything if Firefox is configured correctly for the current profile.
Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.8.3 Disable Java (Level II, Scorable)

Description:
Java is used to load code in the local machine which has more access to the local operating systems as compared to HTML.

Rationale:
This will protect users from loading malicious Java content.

NOTE: This setting will affect applications which rely on Java to run.

Remediation:
Perform the following procedure:

1. Type 'about:config' in the address bar
2. Type security' in the filter
3. Set the preference listed with the values specified below

```
security.enable_java=false
```

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "security.enable_java"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

This will return the following result if Firefox is configured correctly for the current profile.

```
prefs.js:user_pref("security.enable_java", false);
```

Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

2.8.4 Disable Scripting of Plugins by JavaScript (Level I, Scorable)

Description:
Javascript can initiate and interact with the Plug-ins installed in Firefox.

Rationale:
This will protect users from malicious scripts exploiting vulnerabilities in different Plug-ins or abuse the features.

Remediation:
Perform the following procedure:

1. Type 'about:config' in the address bar
2. Type 'Security' in the filter
3. Set the preference listed with the values specified below

```
security.xpconnect.plugin.unrestricted=true
```

Audit:
Perform the following procedure:

1. Close Firefox browser and run the following command:

```
findstr /isl /a:6 "security.xpconnect.plugin.unrestricted"
"%APPDATA%\Mozilla\Firefox\Profiles\*.*"
```

This will not return any results if Firefox is configured correctly for the current profile.
Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed.

Appendix A: References

Resource	Location
[1]. NoScript and Flashblock	https://addons.mozilla.org/en-US/firefox/browse/type:1/cat:12

Appendix B: Change History

Date	Version	Changes for this version
January 7th, 2010	1.0	Public Release