CENTER FOR INTERNET SECURITY

CIS Mozilla Firefox 38 ESR Benchmark

v1.0.0 - 12-31-2015

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

CIS SECURITY BENCHMARKS TERMS OF USE

BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

UNDER THE FOLLOWING TERMS AND CONDITIONS:

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS: CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Table of Contents

Overview

This is the final release of the Mozilla Firefox 38 ESR Benchmark v1.0.0. CIS encourages you to migrate to a more recent, supported version of this technology.

This document provides prescriptive guidance for establishing a secure configuration posture for the Mozilla Firefox 38 ESR Browser. This guide was tested against Mozilla Firefox 38.2.0ESR. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This benchmark 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 the Mozilla Firefox 38 ESR Browser.

Consensus Guidance

This benchmark was created using a consensus review process comprised of 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 published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://community.cisecurity.org.

Typographical 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

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

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

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

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:

Author
Ely Pinto

Contributor
Jordan Rakoske
Blake Frantz
Heather Tarallo

Recommendations

1 Configure Locked Preferences

This section describes how to enable locked preferences for Firefox. The files outlined in this section are used to configure most of the other recommendations listed in this benchmark.

1.1 (L1) Create local-settings.js file (Scored)

Profile Applicability:

- Level 1

Description:

The `local-settings.js` file is used by Firefox to reference and load the `mozilla.cfg` file which contains all the locked preferences.

Rationale:

Loading a custom configuration file is a primary mechanism for setting and enforcing security requirements within Firefox.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `app.update` in the filter
3. Ensure the preferences listed are set to the values specified below

```
general.config.obscure_value=0
general.config.filename=mozilla.cfg
```

Remediation:

Perform the following procedure:

1. Navigate to the `defaults/pref` directory inside the Firefox installation directory and create a file called `local-settings.js`.
2. Include the following lines in `local-settings.js`:

```
pref("general.config.obscure_value", 0);
pref("general.config.filename", "mozilla.cfg");
```

Default Value:

Not configured.

1.2 (L1) Set permissions on local-settings.js (Scored)

Profile Applicability:

- Level 1

Description:

Set permissions on `local-settings.js` so that it can only be modified or deleted by an Administrator.

Rationale:

Any users with the ability to modify the `local-settings.js` file can bypass all security configurations by changing the file or deleting it.

Audit:

Ensure non-administrators do not possess the ability to write to `local-settings.js`.

Remediation:

Deny non-administrators the ability to write to `local-settings.js`.

Default Value:

Not configured.

1.3 (L1) Create mozilla.cfg file (Scored)

Profile Applicability:

- Level 1

Description:

The `mozilla.cfg` file is used by Firefox to configure all the locked preferences.

Rationale:

Loading a custom configuration file is a primary mechanism for setting and enforcing security requirements in Firefox.

Audit:

Perform the following procedure:

1. Navigate to the Firefox installation directory and ensure there is a file called `mozilla.cfg`.
2. Ensure the first line of the file is a comment:

```
//
```

Remediation:

Perform the following procedure:

1. Navigate to the Firefox installation directory and create a file called `mozilla.cfg`.
2. The first line of the file must be a comment:

```
//
```

Default Value:

Not configured.

1.4 (L1) Set permissions on mozilla.cfg (Scored)

Profile Applicability:

- Level 1

Description:

Set permissions on `mozilla.cfg` so that it can only be modified or deleted by an Administrator.

Rationale:

Any users with the ability to modify the `mozilla.cfg` file can bypass all security configurations by changing the file or deleting it.

Audit:

Ensure non-administrators do not possess the ability to write to `mozilla.cfg`.

Remediation:

Deny non-administrators the ability to write to `mozilla.cfg`.

Default Value:

Not configured.

1.5 (L1) Protect Firefox Binaries (Not Scored)

Profile Applicability:

- Level 1

Description:

Ensure that Firefox is installed and owned by an administrative account in order to protect the binaries and to prevent users from circumventing security settings.

Rationale:

When Firefox is installed by an ordinary user, the software in installed into the user's profile / home directory. This avoids the requirement for administrative access during installation and upgrades, but also allows users to circumvent security settings defined in settings.js and mozilla.cfg files. Having the installation owned by an administrative user can also protect binary and configuration files from malware that is executed in an ordinary user's browser.

Audit:

Confirm that Firefox is not installed in any individual user profiles or home directories.

Remediation:

Install Firefox into a shared location that can be accessed by users but modified only by Administrators.

Impact:

Ordinary users will not be able to update or patch Firefox; only Administrators can perform upgrades.

2 Updating Firefox

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

2.1 (L1) Enable Automatic Updates (Scored)

Profile Applicability:

- Level 1

Description:

This feature configures Firefox to automatically download and install updates as they are made available.

Rationale:

Security updates ensure that users are safe from known software bugs and vulnerabilities.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `app.update.auto` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
app.update.enabled=true
app.update.auto=true
app.update.staging.enabled=true
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("app.update.enabled", true);
lockPref("app.update.auto", true);
lockPref("app.update.staging.enabled", true);
```

Default Value:

app.update.enabled=true
app.update.auto=true
app.update.staging.enabled=true

2.2 (L1) Enable Auto-Notification of Outdated Plugins (Scored)

Profile Applicability:

- Level 1

Description:

This feature automatically detects when installed plugins are out of date and notifies the users to update the plugins.

Rationale:

Outdated plugins can be vulnerable or unstable, and can be exploited by malicious websites.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `plugins.update.notifyUser` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
plugins.update.notifyUser=true
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("plugins.update.notifyUser", true);
```

Default Value:

false

2.3 (L1) Enable Information Bar for Outdated Plugins (Scored)

Profile Applicability:

- Level 1

Description:

This feature automatically shows an information bar when installed Plugins are out of date and notifies the users to update the plugins.

Rationale:

Outdated plugins can be vulnerable or unstable, and can be exploited by malicious websites.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `plugins.hide_infobar_for_outdated_plugin` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
plugins.hide_infobar_for_outdated_plugin=false
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("plugins.hide_infobar_for_outdated_plugin", false);
```

Default Value:

false

2.4 (L1) Set Update Interval Time Checks (Scored)

Profile Applicability:

- Level 1

Description:

This configuration sets the amount of time the system waits in between each check for updates.

Rationale:

Frequent checks for updates will mitigate the risk that a system is left vulnerable to known risks for an extended period of time.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `app.update.interval` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
app.update.interval=43200
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("app.update.interval", 43200);
```

Impact:

app.update.enabled must be set to true for this preference to take effect.

Default Value:

43200

2.5 (L1) Set Update Wait Time Prompt (Scored)

Profile Applicability:

- Level 1

Description:

This setting determines the amount of time, in seconds, which the system will wait before displaying the Software Update dialogue box (after an unobtrusive alert has already been shown).

Rationale:

Encouraging the user to update software as soon as possible mitigates the risk that a system will be left vulnerable.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `app.update.promptWaitTime` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
app.update.promptWaitTime=172800
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("app.update.promptWaitTime", 172800);
```

Impact:

1. For this preference to have an effect app.update.enabled must be true and app.update.silent must be false.
2. The full Software Update dialog is still subject toapp.update.idletime.

Default Value:

172800

2.6 (L1) Ensure Update-related UI Components are Displayed (Scored)

Profile Applicability:

- Level 1

Description:

This setting dictates whether the Firefox Update service will notify the user when update related events occur, such as updates being available or downloaded. It is recommended that updated-related notifications be displayed.

Rationale:

Ensuring users are aware of update-related events may reduce the amount of time Firefox remains unpatched.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `app.update.silent` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
app.update.silent=false
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("app.update.silent", false);
```

Default Value:

false

2.7 (L1) Set Search Provider Update Behavior (Scored)

Profile Applicability:

- Level 1

Description:

This feature dictates whether Firefox will update installed search providers. Search providers allow the user to search directly from the "Search bar" which is adjacent to the URL bar.

Rationale:

Software updates help ensure that users are safe from known software bugs and vulnerabilities.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `browser.search.update` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
browser.search.update=true
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("browser.search.update", true);
```

Default Value:

true

3 Network Settings

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

3.1 (L1) Validate Proxy Settings (Not Scored)

Profile Applicability:

- Level 1

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. It 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.

Audit:

Perform the following procedure:

1. Drop down the `Firefox` menu
2. Click on `Options`
3. Select `Options` from the list
4. Click on the `Advanced` Button in the Options window
5. Click on `Network` Tab
6. Click on `Settings` Button
7. Ensure that the proxy listed (if any) is the one configured and approved by the enterprise.

Remediation:

Perform the following procedure:

1. Drop down the `Firefox` menu
2. Click on `Options`

3. Select `Options` from the list
4. Click on the `Advanced` Button in the Options window
5. Click on `Network` Tab
6. Click on `Settings` Button
7. Ensure that the proxy listed (if any) is the one configured and approved by the enterprise.

Default Value:

No proxy.

3.2 (L2) Do Not Send Cross SSL/TLS Referrer Header (Scored)

Profile Applicability:

- Level 2

Description:

This preference dictates whether Firefox will send the URL of the SSL/TLS-protected referring site to the referred SSL/TLS protected site.

Rationale:

The URL of the SSL-protected referring site may contain sensitive information. Preventing this URL from being sent mitigates the risk that the sensitive information will be disclosed.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `network.http.sendSecureXSiteReferrer` in the filter
3. Ensure the preferences listed are set to the values specified below:

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

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("network.http.sendSecureXSiteReferrer", false);
```

Impact:

Enabling this setting may negatively impact the functionality of websites that rely on receiving referrer information.

Default Value:

true

3.3 (L1) Disable NTLM v1 (Scored)

Profile Applicability:

- Level 1

Description:

This feature NT Lan Manager (NTLM) v1 protocol to be used for authentication to resources that request this authentication type.

Rationale:

NTLM v1 contains cryptographic weaknesses that can be easily exploited to obtain user credentials.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `network.auth.force-generic-ntlm-v1` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
network.auth.force-generic-ntlm-v1=false
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("network.auth.force-generic-ntlm-v1", false);
```

Impact:

This may effect websites and browsers that require the use of NTLM v1

Default Value:

false

3.4 (L1) Enable Warning For "Phishy" URLs (Scored)

Profile Applicability:

- Level 1

Description:

It is possible to disguise a website's true location by making use of username/password syntax within the URL (known as "phishy URLs"). This setting will display a warning message whenever a user clicks a link to a phishy URL.

Rationale:

This setting will help protect the browser against phishing.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `network.http.phishy-userpass-length` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
network.http.phishy-userpass-length=1
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("network.http.phishy-userpass-length", 1);
```

Default Value:

1

References:

1. http://dxr.mozilla.org/mozilla-central/search?q=%2Bfunction-ref%3Amozilla%3A%3Anet%3A%3AnsHttpHandler%3A%3APhishyUserPassLength%28%29

3.5 (L2) Enable IDN Show Punycode (Scored)

Profile Applicability:

- Level 2

Description:

This feature determines whether all Internationalized Domain Names (IDNs) displayed in the browser are displayed as Punycode or as Unicode.

Rationale:

IDNs displayed in Punycode are easier to identify and therefore help mitigate the risk of accessing spoofed web pages.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `network.IDN_show_punycode` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
network.IDN_show_punycode=true
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("network.IDN_show_punycode", true);
```

Default Value:

false

3.6 (L1) Set File URI Origin Policy (Scored)

Profile Applicability:

- Level 1

Description:

This feature determines the restrictions placed on the scripts and links loaded into the browser from local HTML files.

Rationale:

Applying the same origin policy to local files will help mitigate the risk of unauthorized access to sensitive information.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `security.fileuri.strict_origin_policy` in the filter
3. Ensure the preferences listed are set to the values specified:

```
security.fileuri.strict_origin_policy=true
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("security.fileuri.strict_origin_policy", true)
```

Default Value:

true

3.7 (L1) Disable Cloud Sync (Scored)

Profile Applicability:

- Level 1

Description:

Firefox allows users to sync preferences and settings, including saved credentials, to cloud-based servers in order to retrieve them from other computers. This setting determines whether cloud sync in enabled.

Rationale:

Disable cloud sync in order to ensure that personal data and credentials are not compromised.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type services.sync.enabled in the filter
3. Ensure the preferences listed are set to the values specified below:

```
services.sync.enabled=false
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("services.sync.enabled", false);
```

Default Value:

true

3.8 (L1) Disable WebRTC (Scored)

Profile Applicability:

- Level 1

Description:

These settings determine whether WebRTC (Web Real Time Communications) is allowed. WebRTC is used for peer to peer communication such as file sharing or video calls.

Rationale:

WebRTC can expose private information such as internal IP addresses and computer settings.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `media.peerconnection` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
media.peerconnection.enabled=false
media.peerconnection.use_document_iceservers=false
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("media.peerconnection.enabled", false);
lockPref("media.peerconnection.use_document_iceservers", false);
```

Default Value:

true

4 Encryption Settings

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

4.1 (L2) Set SSL Override Behavior (Scored)

Profile Applicability:

- Level 2

Description:

When Firefox encounters an invalid certificate and the user clicks "Add Exception", a dialog is displayed with a text box to fetch the certificate from the given URL. This preference controls whether Firefox will or will not automatically fill in the URL text box and auto-fetch the certificate on behalf of the user. Setting this preference to `0` forces the user to enter a URL and click the "Get Certificate" button before adding an exception for an invalid cert.

Rationale:

Requiring the user to manually enter the server's URL and fetch the certificate may provide additional opportunity to scrutinize the certificate before adding an exception for a potentially fraudulent certificate.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `browser.ssl_override_behavior` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
browser.ssl_override_behavior=0
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("browser.ssl_override_behavior", 0);
```

Default Value:

2

4.2 (L1) Set Security TLS Version Maximum (Scored)

Profile Applicability:

- Level 1

Description:

This feature sets the maximum required protocol version.

Rationale:

Setting TLS 1.2 as the maximum authorized protocol version mitigates the risk of using an insecure connection.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `security.tls.version.max` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
security.tls.version.max=3
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("security.tls.version.max", 3)
```

Default Value:

1

4.3 (L1) Set Security TLS Version Minimum (Scored)

Profile Applicability:

- Level 1

Description:

This feature sets the minimum protocol version that may be used when negotiating TLS/SSL sessions.

Rationale:

Setting TLS 1.0 as the minimum protocol version mitigates the risk of negotiating an insecure protocol, such as SSL 2.0.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `security.tls.version.min` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
security.tls.version.min=1
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("security.tls.version.min", 1)
```

Default Value:

0

4.4 (L2) Set OCSP Use Policy (Scored)

Profile Applicability:

- Level 2

Description:

This setting dictates whether Firefox will leverage Online Certificate Status Protocol (OCSP) to determine if a given certificate has been revoked.

Rationale:

Leveraging OCSP may help identify revoked certificates.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `security.OCSP.enabled` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
security.OCSP.enabled=1
```

Note: Configuring this setting to `2` also conforms with this benchmark.

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("security.OCSP.enabled", 1)
```

Impact:

Enabling OCSP carries potential privacy implications. For each HTTPS site Firefox visits, a request is sent to an OCSP server to determine if the site's certificate has been revoked. This provides the OCSP server with the IP address of the requester (Firefox or NAT) and, among other properties, the domain name of the site Firefox is accessing.

Firefox 26 and greater support OCSP Stapling, which mitigates the aforementioned privacy implications of using OCSP.

Default Value:

1

References:

1. https://wiki.mozilla.org/CA:ImprovingRevocation#OCSP_Stapling
2. https://blog.mozilla.org/security/2013/07/29/ocsp-stapling-in-firefox/

4.5 (L1) Block Mixed Active Content (Scored)

Profile Applicability:

- Level 1

Description:

This feature disables the ability to view HTTP content such as JavaScript, CSS, objects, and xhr requests.

Rationale:

Blocking active mixed content minimizes the risk of man-in-the-middle attacks.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `security.mixed_content.block_active_content` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
security.mixed_content.block_active_content=true
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("security.mixed_content.block_active_content", true)
```

Default Value:

true

4.6 (L2) Set OCSP Response Policy (Scored)

Profile Applicability:

- Level 2

Description:

This setting dictates whether Firefox will consider a given certificate to be invalid if Firefox is unable to obtain an Online Certificate Status Protocol (OCSP) response for it.

Rationale:

Requiring an OCSP response will reduce an adversary's ability to successfully leverage a compromised and revoked certificate.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `security.ocsp.require` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
security.ocsp.require=true
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("security.ocsp.require", true);
```

Impact:

Enabling OCSP carries potential privacy implications. For each HTTPS site Firefox visits, a request is sent to an OCSP server to determine if the site's certificate has been revoked. This provides the OCSP server with the IP address of the requester (Firefox or NAT) and, among other properties, the domain name of the site Firefox is accessing.

Additionally, requiring an OCSP response increases opportunity for valid certificates to be deemed invalid. This may occur if OCSP server becomes unavailable or is not accessible.

Firefox 26+ support OCSP Stapling which mitigates the aforementioned privacy implications.

Default Value:

false

References:

1. https://www.grc.com/revocation/ocsp-must-staple.htm
2. https://www.imperialviolet.org/2014/04/19/revchecking.html
3. https://blog.mozilla.org/security/2013/07/29/ocsp-stapling-in-firefox/

5 JavaScript Settings

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

5.1 (L1) Disallow JavaScript's Ability to Change the Status Bar Text (Scored)

Profile Applicability:

- Level 1

Description:

The Status Bar shows the location of the content when a user hovers over 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.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `dom.disable_window_status_change` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
dom.disable_window_status_change=true
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("dom.disable_window_status_change", true);
```

Default Value:

true

5.2 (L1) Disable Scripting of Plugins by JavaScript (Scored)

Profile Applicability:

- Level 1

Description:

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

Rationale:

This may reduce a malicious script's ability to exploit vulnerabilities in plug-ins or abuse plug-in features.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type s`ecurity.xpconnect.plugin.unrestricted` in the filter
3. Set the preference listed with the values specified below:

```
security.xpconnect.plugin.unrestricted=false
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("security.xpconnect.plugin.unrestricted", false);
```

Default Value:

true

5.3 (L1) Disallow JavaScript's Ability to Hide the Address Bar (Scored)

Profile Applicability:

- Level 1

Description:

The Address Bar shows the current URL, which can be used to identify the website.

Rationale:

Some malicious websites can use JavaScript to hide the address bar so that a user cannot determine the URL.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `dom.disable_window_open_feature.location` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
dom.disable_window_open_feature.location=true
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("dom.disable_window_open_feature.location", true);
```

Default Value:

true

5.4 (L1) Disallow JavaScript's Ability to Hide the Status Bar (Scored)

Profile Applicability:

- Level 1

Description:

The 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.

Audit:

Perform the following procedure:

1. Type `about.config` in the address bar
2. Type `dom.disable_window_open_feature.status` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
dom.disable_window_open_feature.status=true
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("dom.disable_window_open_feature.status", true);
```

Default Value:

true

5.5 (L1) Disable Closing of Windows via Scripts (Scored)

Profile Applicability:

- Level 1

Description:

Firefox can be configured to prevent scripts 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.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `dom.allow_scripts_to_close_windows` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
dom.allow_scripts_to_close_windows=false
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("dom.allow_scripts_to_close_windows", false);
```

Default Value:

false

5.6 (L1) Block Pop-up Windows (Scored)

Profile Applicability:

- Level 1

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.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `privacy.popups.policy` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
privacy.popups.policy=1
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("privacy.popups.policy", 1);
```

Default Value:

1

5.7 (L1) Disable Displaying JavaScript in History URLs (Scored)

Profile Applicability:

- Level 1

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.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `browser.urlbar.filter.javascript` in the filter
3. Ensure the preferences listed are set to the values specified below:

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

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("browser.urlbar.filter.javascript", true);
```

Default Value:

true

6 Privacy Settings

This sections contains recommendations pertaining largely to privacy as it relates to browsing behaviors. While Firefox contains several settings that allow a user to sanitize and/or avoid persisting browsing artifacts, such as download history, caches, form data, etc, this section does not contain recommendations for configuring such settings. Users concerned with the privacy implications of such artifacts are encouraged to browse in a "Private Window". For more information on private browsing in Firefox, please see: https://support.mozilla.org/en-US/kb/private-browsing-browse-web-without-saving-info.

6.1 (L1) Disallow Credential Storage (Scored)

Profile Applicability:

- Level 1

Description:

Firefox allows credentials to be stored for certain websites.

Rationale:

Stored credentials may be harvested by an adversary that gains local privileges equal to or greater than the principal running Firefox, which may increase the scope and impact of a breach. However, preventing Firefox from storing credentials will not prevent such an adversary from harvesting credentials used while compromised.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type signon.rememberSignons in the filter
3. Ensure the preferences listed are set to the values specified below:

```
signon.rememberSignons=false
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

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

Default Value:

true

6.2 (L1) Do Not Accept Third Party Cookies (Scored)

Profile Applicability:

- Level 1

Description:

A third-party cookie is a cookie sent by a domain that differs from the domain in the browser's address bar.

Rationale:

Third party cookies are often used for tracking user browsing behaviors, which has privacy implications. However, preventing third-party cookies does not completely mitigate privacy concerns as several other active tracking mechanisms exist[1].

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `network.cookie.cookieBehavior` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
network.cookie.cookieBehavior=1
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

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

Impact:

Blocking third-party cookies may adversely effect the functionality of some sites.

Default Value:

0

References:

1. https://github.com/samyk/evercookie

6.3 (L1) Tracking Protection (Scored)

Profile Applicability:

- Level 1

Description:

These settings instruct the browser to communicate the preference not to be tracked to websites to which it connects, and additionally attempt to block tracking.

Rationale:

Enabling Do Not Track instructs the browser to send an optional header in HTTP requests made from the app that indicates a preference not to be tracked by websites. This optional header is voluntary in nature, having no method to enforce adherence and providing no guarantee that web sites will honor the preference. However, a large number of websites do honor it so there is privacy benefit in enabling it.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `track` in the filter
3. Ensure the preferences listed are set to the values specified below:

   privacy.donottrackheader.enabled=true
   privacy.donottrackheader.value=1
   privacy.trackingprotection.enabled=true
   privacy.trackingprotection.pbmode=true

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

   lockPref("privacy.donottrackheader.enabled", true);
   lockPref("privacy.donottrackheader.value", 1);
   lockPref("privacy.trackingprotection.enabled ", true);
   lockPref("privacy.trackingprotection.pbmode", true);

Default Value:

privacy.donottrackheader.enabled=false

privacy.donottrackheader.value=1

privacy.trackingprotection.enabled = false

privacy.trackingprotection.pbmode = false

6.4 (L1) Set Delay for Enabling Security Sensitive Dialog Boxes (Scored)

Profile Applicability:

- Level 1

Description:

This feature sets the amount of time in milliseconds that elapse before the buttons on security-sensitive dialog boxes are enabled.

Rationale:

This delay help prevents Firefox users from inadvertently installing malicious software.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `security.dialog_enable_delay` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
security.dialog_enable_delay=2000
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("security.dialog_enable_delay", 2000);
```

Default Value:

2000

References:

1. http://www.squarefree.com/2004/07/01/race-conditions-in-security-dialogs/

6.5 (L1) Disable Geolocation Serivces (Scored)

Profile Applicability:

- Level 1

Description:

This settings determines whether Firefox will provide geographic location information to websites.

Rationale:

Geo-location services can expose private information to remote websites.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `geo.enabled` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
geo.enabled=false
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("geo.enabled", false);
```

Default Value:

true

7 Extensions and Add-ons

This sections contains recommendations related to how Firefox manages extensions and add-ons.

7.1 (L1) Secure Application Plug-ins (Scored)

Profile Applicability:

- Level 1

Description:

Some active content such as audio and video can be automatically loaded by Firefox on websites. It is recommended to secure application plug-ins.

Rationale:

Some malicious websites use active content to exploit vulnerabilities in the active content handling application plug-in. It is recommended to always prompt the user when a website is about to load active content.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `browser.helperApps.alwaysAsk.force` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
browser.helperApps.alwaysAsk.force=true
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("browser.helperApps.alwaysAsk.force", true);
```

Default Value:

false

7.2 (L1) Disabling Auto-Install of Add-ons (Scored)

Profile Applicability:

- Level 1

Description:

This configuration will show how to ensure that no website is allowed to automatically install Add-Ons. 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.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `xpinstall.whitelist.required` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
xpinstall.whitelist.required=true
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("xpinstall.whitelist.required", true);
```

Default Value:

true

7.3 (L1) Enable Extension Block List (Scored)

Profile Applicability:

- Level 1

Description:

This feature enables Mozilla to retrieve a list of blocked applications from the server.

Rationale:

Enabling Mozilla to access the list of blocked applications mitigates the risk of installing a known malicious application.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `extensions.blocklist.enabled` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
extensions.blocklist.enabled=true
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("extensions.blocklist.enabled", true);
```

Default Value:

true

7.4 (L1) Set Extension Block List Interval (Scored)

Profile Applicability:

- Level 1

Description:

This feature determines how often Mozilla will attempt to retrieve a list of blocked applications from the server.

Rationale:

An updated list of blocked applications mitigates the risk of installing and using a known malicious application.

Audit:

Perform the following procedure:

1. Type about:config in the address bar
2. Type extension.blocklist.interval in the filter
3. Ensure the preferences listed are set to the values specified below:

```
extensions.blocklist.interval=86400
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("extensions.blocklist.interval", 86400);
```

Default Value:

86400

7.5 (L1) Enable Warning for External Protocol Handler (Scored)

Profile Applicability:

- Level 1

Description:

This feature indicates whether the user is warned before opening an external application for pre-configured protocols were its behavior is undefined.

Rationale:

Enabling a warning to appear before passing data to an external application mitigates the risk that sensitive information will be made vulnerable to outside threats.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `network.protocol-handler.warn-external-default` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
network.protocol-handler.warn-external-default=true
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("network.protocol-handler.warn-external-default", true);
```

Default Value:

true

7.6 (L1) Disable Popups Initiated by Plugins (Scored)

Profile Applicability:

- Level 1

Description:

This feature controls popups that are initiated by plugins.

Rationale:

Disabling plugin popups (except from white-listed sites) from being displayed, guard a user against any attacks launched using a Pop-up.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `privacy.popups.disable_from_plugins` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
privacy.popups.disable_from_plugins=2
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("privacy.popups.disable_from_plugins", 2)
```

Default Value:

2

7.7 (L1) Enable Extension Auto Update (Scored)

Profile Applicability:

- Level 1

Description:

This feature configures Firefox to automatically download and install updates as they are made available.

Rationale:

Security updates ensure that users are safe from known software bugs and vulnerabilities.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `extensions.update.autoUpdateDefault` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
extensions.update.autoUpdateDefault=true
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("extensions.update.autoUpdateDefault", true)
```

Default Value:

true

7.8 (L1) Enable Extension Update (Scored)

Profile Applicability:

- Level 1

Description:

This feature configures Firefox to prompt when updates are made available.

Rationale:

Security updates ensure that users are safe from known software bugs and vulnerabilities.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `extensions.update.enabled` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
extensions.update.enabled=true
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("extensions.update.enabled", true)
```

Default Value:

true

7.9 (L1) Set Extension Update Interval Time Checks (Scored)

Profile Applicability:

- Level 1

Description:

This feature sets the amount of time the system waits between checking for updates.

Rationale:

Setting a specific amount of time between automatically checking for updates mitigates the risk that a system will left vulnerable to known risks for an extended period of time.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `extensions.update.interval` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
extensions.update.interval=86400
```

Note: A value less than `86400` is in conformance with this benchmark.

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("extensions.update.interval", 86400)
```

Default Value:

86400

8 Malware Settings

This sections contains recommendations for configuring FireFox's malware-related settings.

8.1 (L1) Enable Virus Scanning for Downloads (Scored)

Profile Applicability:

- Level 1

Description:

This feature configures the browser to scan downloads for viruses.

Rationale:

This will ensure that a downloaded file is scanned for viruses before the user has an opportunity to interact with the download. It will also ensure that Windows Policy for downloaded files is followed properly.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `browser.download.manager.scanWhenDone` in the filter
3. Ensure the preferences listed are set to the values specified below:

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

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("browser.download.manager.scanWhenDone", true);
```

Default Value:

true

8.2 (L1) Disable JAR from Opening Unsafe File Types (Scored)

Profile Applicability:

- Level 1

Description:

This feature gives the user the ability to override the restriction on only loading files with `application/java-archive` or `application/x-jar` content types.

Rationale:

Enabling the browser to only load `application/java-archive` or `application/x-jar` content types mitigates the risk of malware infection and other attack vectors.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `network.jar.open-unsafe-types` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
network.jar.open-unsafe-types=false
```

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("network.jar.open-unsafe-types", false);
```

Default Value:

false

8.3 (L1) Block Reported Web Forgeries (Scored)

Profile Applicability:

- Level 1

Description:

This feature alerts the user if they are visiting a known phishing website.

Rationale:

Enabling this feature helps mitigate the threat of phishing attacks.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `browser.safebrowsing.enabled` in the filter
3. Ensure the preferences listed are set to the values specified below:

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

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("browser.safebrowsing.enabled", true);
```

Default Value:

true

8.4 (L1) Block Reported Attack Sites (Scored)

Profile Applicability:

- Level 1

Description:

This feature alerts the user if they are visiting a known malicious website.

Rationale:

Enabling this feature will decrease the probability of a user falling victim to a known malicious web site.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar
2. Type `browser.safebrowsing.malware.enabled` in the filter
3. Ensure the preferences listed are set to the values specified below:

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

Remediation:

Perform the following procedure:

1. Open the `mozilla.cfg` file in the installation directory with a text editor
2. Add the following lines to `mozilla.cfg`:

```
lockPref("browser.safebrowsing.malware.enabled", true);
```

Default Value:

true

Control		Set Correctly	
		Yes	No
1	**Configure Locked Preferences**		
1.1	(L1) Create local-settings.js file (Scored)	☐	☐
1.2	(L1) Set permissions on local-settings.js (Scored)	☐	☐
1.3	(L1) Create mozilla.cfg file (Scored)	☐	☐
1.4	(L1) Set permissions on mozilla.cfg (Scored)	☐	☐
1.5	(L1) Protect Firefox Binaries (Not Scored)	☐	☐
2	**Updating Firefox**		
2.1	(L1) Enable Automatic Updates (Scored)	☐	☐
2.2	(L1) Enable Auto-Notification of Outdated Plugins (Scored)	☐	☐
2.3	(L1) Enable Information Bar for Outdated Plugins (Scored)	☐	☐
2.4	(L1) Set Update Interval Time Checks (Scored)	☐	☐
2.5	(L1) Set Update Wait Time Prompt (Scored)	☐	☐
2.6	(L1) Ensure Update-related UI Components are Displayed (Scored)	☐	☐
2.7	(L1) Set Search Provider Update Behavior (Scored)	☐	☐
3	**Network Settings**		
3.1	(L1) Validate Proxy Settings (Not Scored)	☐	☐
3.2	(L2) Do Not Send Cross SSL/TLS Referrer Header (Scored)	☐	☐
3.3	(L1) Disable NTLM v1 (Scored)	☐	☐
3.4	(L1) Enable Warning For "Phishy" URLs (Scored)	☐	☐
3.5	(L2) Enable IDN Show Punycode (Scored)	☐	☐
3.6	(L1) Set File URI Origin Policy (Scored)	☐	☐
3.7	(L1) Disable Cloud Sync (Scored)	☐	☐
3.8	(L1) Disable WebRTC (Scored)	☐	☐
4	**Encryption Settings**		
4.1	(L2) Set SSL Override Behavior (Scored)	☐	☐
4.2	(L1) Set Security TLS Version Maximum (Scored)	☐	☐
4.3	(L1) Set Security TLS Version Minimum (Scored)	☐	☐
4.4	(L1) Set OCSP Use Policy (Scored)	☐	☐
4.5	(L1) Block Mixed Active Content (Scored)	☐	☐
4.6	(L1) Set OCSP Response Policy (Scored)	☐	☐
5	**JavaScript Settings**		
5.1	(L1) Disallow JavaScript's Ability to Change the Status Bar Text (Scored)	☐	☐
5.2	(L1) Disable Scripting of Plugins by JavaScript (Scored)	☐	☐
5.3	(L1) Disallow JavaScript's Ability to Hide the Address Bar (Scored)	☐	☐
5.4	(L1) Disallow JavaScript's Ability to Hide the Status Bar (Scored)	☐	☐
5.5	(L1) Disable Closing of Windows via Scripts (Scored)	☐	☐
5.6	(L1) Block Pop-up Windows (Scored)	☐	☐

5.7	(L1) Disable Displaying JavaScript in History URLs (Scored)	☐	☐
6	**Privacy Settings**		
6.1	(L1) Disallow Credential Storage (Scored)	☐	☐
6.2	(L1) Do Not Accept Third Party Cookies (Scored)	☐	☐
6.3	(L1) Tracking Protection (Scored)	☐	☐
6.4	(L1) Set Delay for Enabling Security Sensitive Dialog Boxes (Scored)	☐	☐
6.5	(L1) Disable Geolocation Serivces (Scored)	☐	☐
7	**Extensions and Add-ons**		
7.1	(L1) Secure Application Plug-ins (Scored)	☐	☐
7.2	(L1) Disabling Auto-Install of Add-ons (Scored)	☐	☐
7.3	(L1) Enable Extension Block List (Scored)	☐	☐
7.4	(L1) Set Extension Block List Interval (Scored)	☐	☐
7.5	(L1) Enable Warning for External Protocol Handler (Scored)	☐	☐
7.6	(L1) Disable Popups Initiated by Plugins (Scored)	☐	☐
7.7	(L1) Enable Extension Auto Update (Scored)	☐	☐
7.8	(L1) Enable Extension Update (Scored)	☐	☐
7.9	(L1) Set Extension Update Interval Time Checks (Scored)	☐	☐
8	**Malware Settings**		
8.1	(L1) Enable Virus Scanning for Downloads (Scored)	☐	☐
8.2	(L1) Disable JAR from Opening Unsafe File Types (Scored)	☐	☐
8.3	(L1) Block Reported Web Forgeries (Scored)	☐	☐
8.4	(L1) Block Reported Attack Sites (Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
2015/12/31	1.0.0	Based off 24 ESR build v1.0.0
2015/12/31	1.0.0	1 Updating Firefox - Include search plugins - Ticket #45
2015/12/31	1.0.0	2 Network Settings - Include IDN settings - Ticket #48
2015/12/31	1.0.0	Network.protocol-handler.external.* - Include in benchmark – Ticket #51
2015/12/31	1.0.0	Privacy.clearOnShutdown.* & privacy.sanitize.sanitizeOnShutdown – Ticket #54
2015/12/31	1.0.0	3.5 Set Network Cookie Behavior – Ticket #59
2015/12/31	1.0.0	network.negotiate-auth.allow-insecure-ntlm-v1 (Deny NTLMv1 over http) – Ticket #68
2015/12/31	1.0.0	3.3 Disable NTLM v1 – Ticket #70
2015/12/31	1.0.0	3.4 Disable Sending LM Hash – Ticket #71
2015/12/31	1.0.0	5.3 Disallow JavaScript's Ability to Hide the Address Bar – Ticket #72
2015/12/31	1.0.0	7.1 this menu option doesn't exist anymore – Ticket #73