CENTER FOR INTERNET SECURITY

CIS Mozilla Firefox 24 ESR Benchmark

v1.0.0 - 04-28-2014

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 document provides prescriptive guidance for establishing a secure configuration posture for the Mozilla Firefox 24 ESR Browser. This guide was tested against Mozilla Firefox 24 ESR and Mozilla Firefox 24.4 ESR. 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 24 ESR Browser.

Consensus Guidance

This benchmark was created using a consensus review process comprised 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:

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 Create the 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 required in order to set security recommendations.

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 Set permissions on local-settings.js (Not Scored)

Profile Applicability:

- Level 1

Description:

Set permissions on the local-settings.js file 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 that the local-settings.js file is read-only using tools provided by the host Operating Systems. Only administrators should be able to modify the file.

Remediation:

Mark the file and parent directories as read-only using tools provided by the host Operating Systems. Only administrators should be able to modify the file.

Default Value:

Not configured.

1.3 Create the mozilla.cfg file (Not 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 required in order to set security recommendations.

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:
3. `//`

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:
3. `//`

Default Value:

Not configured.

1.4 Set permissions on mozilla.cfg (Not Scored)

Profile Applicability:

- Level 1

Description:

Set permissions on the local-settings.js file 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 that the local-settings.js file is read-only using tools provided by the host Operating Systems. Only administrators should be able to modify the file.

Remediation:

Mark the mozilla.cfg file and parent directories as read-only using tools provided by the host Operating Systems. Only administrators should be able to modify the file.

Default Value:

Not configured.

2 Updating Firefox

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

2.1 Enable Software Updates (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 `app.update.enabled` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
app.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("app.update.enabled", "true")
```

2.2 Enable 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 `app.update.auto` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
app.update.auto=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.auto", true);
```

Default Value:

Enabled.

2.3 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:

Disabled.

2.4 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:

Enabled.

2.5 Set Auto-Update Channel (Scored)

Profile Applicability:

- Level 2

Description:

This feature determines the type of builds auto-update will look for.

Rationale:

Installing updates for incompatible builds can cause system instability.

Audit:

Perform the following procedure:

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

```
app.update.channel=esr
```

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.channel", "esr");
```

2.6 Set Update URL (Scored)

Profile Applicability:

- Level 1

Description:

This feature determines the URL used when checking for updates.

Rationale:

Setting the incorrect URL for auto-update leaves the system at risk since patches and bug-fixes will not be installed.

Audit:

Perform the following procedure:

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

```
app.update.url=https://aus3.mozilla.org/update/3/%PRODUCT%/%VERSION%/%BUILD_ID%
/%BUILD_TARGET%/%LOCALE%/%CHANNEL%/%OS_VERSION%/%DISTRIBUTION%/%DISTRIBUTION_VE
RSION%/update.xml
```

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.url",
"https://aus3.mozilla.org/update/3/%PRODUCT%/%VERSION%/%BUILD_ID%/%BUILD_TARGET
%/%LOCALE%/%CHANNEL%/%OS_VERSION%/%DISTRIBUTION%/%DISTRIBUTION_VERSION%/update.
xml");
```

2.7 Set Update Detail URL (Scored)

Profile Applicability:

- Level 1

Description:

This feature sets a default URL for accessing more information about an update when an individual link is not provided by the update.

Rationale:

An undefined link could be set to send a user to a malicious website.

Audit:

Perform the following procedure:

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

```
app.update.url.details=https://www.mozilla.org/%LOCALE%/firefox/notes
```

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.url.details",
"https://www.mozilla.org/%LOCALE%/firefox/notes");
```

2.8 Set Manual Update URL (Scored)

Profile Applicability:

- Level 1

Description:

This feature sets the URL where a user can manually download and install updates if the auto-update feature fails.

Rationale:

An undefined link could be set to send a user to a malicious website.

Audit:

Perform the following procedure:

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

```
app.update.url.manual=https://www.mozilla.org/firefox/
```

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.url.manual", "https://www.mozilla.org/firefox/");
```

2.9 Set Update Idle Time (Scored)

Profile Applicability:

- Level 1

Description:

The feature sets a default amount of time the browser has to be idle before displaying a dialogue box indicating a software update is available.

Rationale:

A dialogue box indicating a software update risks being accidentally closed if it is displayed while a user is actively engaged with their browser.

Audit:

Perform the following procedure:

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

```
app.update.idletime=60
```

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.idletime", "60");
```

2.10 Set Update Mode Compatibility (Scored)

Profile Applicability:

- Level 1

Description:

This feature determines if a user will be informed of compatible updates for incompatible extensions and/or themes after a software update occurs.

Rationale:

Incompatible extensions and/or themes could cause system instability and/or a malicious intrusion point.

Audit:

Perform the following procedure:

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

```
app.update.incompatible.mode=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("app.update.incompatible.mode", "1");
```

Impact:

For this preference to have an effect app.update.enabled must be true
and app.update.silent must be false.

2.11 Configure for Update Verification (Scored)

Profile Applicability:

- Level 1

Description:

This feature displays a dialogue box indicating a successful software update once a system has been restarted.

Rationale:

The indication of a successful software update prevents updates that were not installed successfully from going unnoticed and therefore mitigating the risk of an unknowingly vulnerable system.

Audit:

Perform the following procedure:

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

```
app.update.showInstallUI=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.showInstallUI", "true");
```

Impact:

To download updates app.update.enabled must be set to true.

2.12 Set Update Wait Time Prompt (Scored)

Profile Applicability:

- Level 1

Description:

This feature sets the amount of time the system waits after displaying an unobtrusive alert indicating a software update before showing the Software Update dialogue box.

Rationale:

Setting a window of time between a software update alert and showing the Software Update dialogue box mitigates the risk that a user will cancel and/or ignore both software update indications. This 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=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.promptWaitTime", "43200");
```

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.

2.13 Set 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 `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.

2.14 Disable Update Silencing (Scored)

Profile Applicability:

- Level 1

Description:

This feature disables all UI prompting of software updates.

Rationale:

Disabling UI software update prompts creates the risk that a system will be left open to known vulnerabilities through lack of timely software patches.

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");
```

Impact:

For this preference to have an effect app.update.enabled must be true.

2.15 Set Update Mode (Scored)

Profile Applicability:

- Level 1

Description:

This feature designates which updates are downloaded in the background and which require a user prompt to be applied.

Rationale:

Prompting a user to acknowledge updates with known extension incompatibilities mitigates the risk that a system will be left unstable and/or vulnerable.

Audit:

Perform the following procedure:

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

```
app.update.mode=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("app.update.mode", "1")
```

3 Network Settings

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

3.1 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 Disable Referrer from an SSL Website (Scored)

Profile Applicability:

- Level 1

Description:

This feature provides a referred site with the URL of the referring 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);
```

Default Value:

True.

3.3 Enable Warning For "Phishy" URLs (Scored)

Profile Applicability:

- Level 1

Description:

This feature enables the leveraging of the Microsoft Windows Security Support Provider Interface (SSPI).

Rationale:

This will protect users against weaker authentication.

Audit:

Perform the following procedure:

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

```
network.auth.use-sspi=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.auth.use-sspi", true);
```

Impact:

This setting is only required for Microsoft Windows operating systems.

Default Value:

1.

3.4 Enable SSPI Authentication (Scored)

Profile Applicability:

- Level 1

Description:

This feature enables the leveraging of the Microsoft Windows Security Support Provider Interface (SSPI).

Rationale:

This will protect users against weaker authentication.

Audit:

Perform the following procedure:

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

```
network.auth.use-sspi=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.auth.use-sspi", true);
```

Impact:

This setting is only required for Microsoft Windows operating systems.

Default Value:

True (Microsoft Windows operating systems).

False (All other operating systems).

3.5 Disable Sending LM Hash (Scored)

Profile Applicability:

- Level 1

Description:

This feature allows for a LM Hash to be sent when authenticating to resources that request this authentication type.

Rationale:

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

Audit:

Perform the following procedure:

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

```
network.ntlm.send-lm-response=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.ntlm.send-lm-response", false);
```

Default Value:

False.

3.6 Set Network Cookie Behavior (Scored)

Profile Applicability:

- Level 1

Description:

This feature sets the types of cookies allowed by the browser.

Rationale:

Third party cookies are often used for tracking user behavior and collecting information about users, such as viewing habits, preferences, and configuration settings.

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:

Changing this setting may adversely affect certain websites.

Default Value:

0

3.7 Enable the Retention of Third-Party Cookies during Current Session (Scored)

Profile Applicability:

- Level 1

Description:

This feature decides whether the browser retains third-party cookies after a session has ended.

Rationale:

Third party cookies are often used for tracking user behavior and collecting information about users, such as viewing habits, preferences, and configuration settings.

Audit:

Perform the following procedure:

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

```
network.cookie.thirdparty.sessionOnly=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.cookie.thirdparty.sessionOnly", "true");
```

3.8 Disable Send Referrer Header (Scored)

Profile Applicability:

- Level 1

Description:

This feature indicates when the Referrer header is to be sent and sets `document.referrer`.

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.sendRefererHeader` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
network.http.sendReferer.Header=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("network.http.sendRefererHeader", "0");
```

3.9 Enable IDN Show Punycode (Scored)

Profile Applicability:

- Level 1

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");
```

3.10 Set IDN Blacklist Characters (Scored)

Profile Applicability:

- Level 1

Description:

This feature creates a blacklist of Unicode characters that cannot be used within an IDN. If an IDN contains on the characters the IDN is automatically changed from Unicode to Punycode.

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.blacklist_chars` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
network.IDN.blacklist_chars= ¼½¾Çƒ•Ì·Ì¸Ö‰×ƒ×´Ø‰ØŠÙªÛ”Ü□Ü,ÜƒÜ„á…Ÿá… áœµâ€€â€•
â€„â€…â€†â€‡â€ˆâ€Šâ€¤â€§â€¨â€©â€¯‹ ›â••⁄â□’â□Ÿâ…“â…”â…•â…–â…—
â…˜â…™â…šâ…›â…œâ…□â…žâ…Ÿâ^•â^¶âŽ®â•±â§¶â§¸â«»â«½â¿°â¿±â¿²â¿³â¿´â¿µâ¿¶â¿·â¿¸â¿¹â
```

```
¿°â¿»ã€€ã€‚ã€”ã€•ã€³ã…¤ãˆ•ãˆžãŽ®ãŽ¯ã•†ã□Ÿêž‰ï¸”ï¸•ï¸¿ï¹□ï¹žï¼Žï¼¿□ï¹½¡ï¾ ï¿¹ï¿°ï¿
»ï¿¼ï¿½
```

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.blacklist_chars", "
¼½¾ÇƒË•Ì·Ì¸Ö‰×ƒ×´Ø‰ØŠÙªÛ”Ü□Ü,ÜƒÜ„á…Ÿá… áœµâ€€â€•
â€„â€…â€†â€‡â€ˆ â€Šâ€¤â€§â€¨â€©â€¯‹ ›â••⁄â□′â□Ÿâ…“â…”â….•â….–â…—
â…˜â…™â…šâ…› ›â…œâ…□â…žâ…Ÿâˆ•â^¶âŽ®â•±â§¶â§¸â«»â«½â¿°â¿±â¿²â¿³â¿´â¿µâ¿¶â¿·â¿¸â¿¹â
¿°â¿»ã€€ã€‚ã€”ã€•ã€³ã…¤ãˆ□ãˆžãŽ®ãŽ¯ã□†ã□Ÿêž‰ï¸”ï¸•ï¸¿ï¹□ï¹žï¼Žï¼¿•ï¹½¡ï¾ ï¿¹ï¿°ï¿
»ï¿¼ï¿½");
```

3.11 Set IDN Whitelist (Scored)

Profile Applicability:

- Level 1

Description:

This feature creates a whitelist of IDN addresses that contain blacklisted Unicode characters but are allowed to be displayed as intended due to the IDN's public anti-spoofing policy.

Rationale:

The threat of accessing a spoofed website is greatly mitigated by the whitelisted IDN's adherence to their public anti-spoofing policy.

Audit:

Perform the following procedure:

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

```
network.IDN.whitelist.*=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.whitelist.*", "true");
```

Impact:

As this is a whitelist and not a blacklist, setting any of these preferences to false is the same as not setting the preference at all.

3.12 Disable Auto Authentication with Proxy Servers (Scored)

Profile Applicability:

- Level 1

Description:

This feature determines whether to automatically authenticate the user via NTLM, using their Windows domain logon, with proxy servers.

Rationale:

Disabling automatic authentication mitigates the risk of a user unknowingly connecting to an un-trusted server.

Audit:

Perform the following procedure:

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

```
network.automatic-ntlm-auth.allow-proxies=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.automatic-ntlm-auth.allow-proxies", "false");
```

3.13 Set Trusted Sites for NTLM Auto Authentication (Scored)

Profile Applicability:

- Level 1

Description:

This feature sets which sites are allowed to automatically authenticate via NTLM.

Rationale:

Setting a list of trusted sits to automatically authenticate mitigates the risk of a user being connected to an unknown server without their consent and/or accepting the prompt of an un-trusted server accidentally.

Audit:

Perform the following procedure:

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

```
network.automatic-ntlm-auth.trusted-uris=
```

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.automatic-ntlm-auth.trusted-uris", "");
```

3.14 Disable Auto Acceptance of Session Cookies (Scored)

Profile Applicability:

- Level 1

Description:

This feature sets whether session cookies are automatically accepted.

Rationale:

Disabling the automatic acceptance of session cookies mitigates the risk that a user's browser movements and behavior will be monitored.

Audit:

Perform the following procedure:

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

```
network.cookie.alwaysAcceptSessionCookies=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.cookie.alwaysAcceptSessionCookies", "false");
```

3.16 Set Cookie Lifetime Policy (Scored)

Profile Applicability:

- Level 1

Description:

This feature sets how long cookies are stored before deletion.

Rationale:

Setting all cookies to be deleted upon closing the browser mitigates the risk of a user's browser activities being discovered.

Audit:

Perform the following procedure:

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

```
network.cookie.lifetimePolicy=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("network.cookie.lifetimepolicy", "2");
```

3.18 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 cross-site scripting issues on secure sites.

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");
```

3.20 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");
```

3.21 Set Network Proxy URL (Scored)

Profile Applicability:

- Level 1

Description:

This setting allows a proxy URL to be defined.

Rationale:

Defining a proxy URL mitigates the risk of connecting to an untrusted proxy server.

Audit:

Perform the following procedure:

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

```
network.proxy.autoconfig_url=
```

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.proxy.autoconfig_url", "");
```

3.23 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")
```

4 Encryption Settings

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

4.1 Set SSL Override Behavior (Scored)

Profile Applicability:

- Level 2

Description:

This feature determines whether SSL certificate errors can be overridden.

Rationale:

Not allowing the system to pre-populate the URL or pre-fetch the security certificate mitigates the risk of connecting to a malicious website.

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");
```

4.2 Set Security TLS Version Minimum (Scored)

Profile Applicability:

- Level 1

Description:

This feature sets the minimum required protocol version.

Rationale:

Setting SSL 3.0 as the minimum 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.min` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
security.tls.version.min=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("security.tls.version.min", "0")
```

4.3 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")
```

4.4 Enable Security OCSP (Scored)

Profile Applicability:

- Level 1

Description:

This feature sets the behavior of OCSP-based certificate verification and validation.

Rationale:

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

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=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("security. OCSP. enabled", "2")
```

4.5 Enable Require OCSP (Scored)

Profile Applicability:

- Level 1

Description:

This feature automatically terminates the connection to a website with a revoked certificate.

Rationale:

Enabling OCSP require minimizes the risk of continuing to visit a website with an invalid 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");
```

4.6 Block Active Mixed 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")
```

5 JavaScript Settings

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

5.1 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");
```

5.2 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 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.

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");
```

5.3 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 will protect users from malicious scripts exploiting vulnerabilities in different Plug-ins or abuse the 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");
```

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

Profile Applicability:

- Level 1

Description:

The Address Bar shows the current URL.

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

5.7 Disable Closing of Windows via Scripts (Scored)

Profile Applicability:

- Level 1

Description:

Firefox can be configured to prevent script 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");
```

5.8 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");
```

5.9 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");
```

6 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.

6.1 Disallow Credential Storage (Scored)

Profile Applicability:

- Level 1

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.

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");
```

6.2 Disable Prompting for Credential Storage (Scored)

Profile Applicability:

- Level 2

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.

Audit:

Perform the following procedure:

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

```
security.ask_for_password=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("security.ask_for_password", "0");
```

6.3 Delete Download History (Scored)

Profile Applicability:

- Level 2

Description:

Firefox can store downloads from Internet resources.

Rationale:

If Firefox or other applications executing at equal or higher security contexts is compromised, potentially sensitive, persisted, form data is at increased risk.

Audit:

Perform the following procedure:

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

```
browser.download.manager.retention=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.download.manager.retention", "0");
```

6.4 Delete Search and Form History (Scored)

Profile Applicability:

- Level 2

Description:

Firefox can store Search and Form Data from Internet resources.

Rationale:

If Firefox or other applications executing at equal or higher security contexts is compromised, potentially sensitive, persisted, form data is at increased risk.

Audit:

Perform the following procedure:

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

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

6.5 Clear SSL Form Session Data (Scored)

Profile Applicability:

- Level 2

Description:

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

Rationale:

If Firefox or other applications executing at equal or higher security contexts is compromised, potentially sensitive, persisted, form data is at increased risk.

Audit:

Perform the following procedure:

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

```
browser.sessionstore.privacy_level=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("browser.sessionstore.privacy_level", "1")
```

6.6 Disable Caching of SSL Pages (Scored)

Profile Applicability:

- Level 1

Description:

Firefox can locally cache the content of SSL pages on disk.

Rationale:

This will protect user s confidential information from unauthorized disclosure.

Audit:

Perform the following procedure:

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

```
browser.cache.disk_cache_ssl=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("browser.cache.disk_cache_ssl", "false");
```

6.7 Disable Form Auto-Fill (Scored)

Profile Applicability:

- Level 1

Description:

This feature disables Firefox from saving and automatically filling in usernames and passwords.

Rationale:

Disabling Form Auto-Fill mitigates the risk of usernames and passwords being exposed via cross-site forms.

Audit:

Perform the following procedure:

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

```
signon.autofillForms=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.autofillForms", "false");
```

6.8 Disable Third Party Browser Tracking (Scored)

Profile Applicability:

- Level 1

Description:

This feature opts out of third-party tracking of browser behavior.

Rationale:

Enabling Do Not Track Header mitigates the risk of malicious actors gathering information on a user's browsing patterns.

Audit:

Perform the following procedure:

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

```
privacy.donottrackheader.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("privacy.donottrackheader.enabled", "true");
```

6.9 Set Do Not Track Header Value (Not Scored)

Profile Applicability:

- Level 1

Description:

This feature opts out of third-party browser tracking.

Rationale:

Enabling Do Not Track Header mitigates the risk of malicious actors gathering information on a user's browsing patterns.

Audit:

Perform the following procedure:

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

```
privacy.donottrackheader.value=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.donottrackheader.value", "1")
```

6.10 Enable Sanitize on Shutdown (Scored)

Profile Applicability:

- Level 1

Description:

This feature initiates Clear Private Data whenever the browser is closed.

Rationale:

Sanitize on shutdown mitigates the risk of sensitive user data being compromised.

Audit:

Perform the following procedure:

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

```
privacy.sanitize.sanitizeOnShutDown=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.sanitize.sanitizeOnShutDown", "true")
```

6.11 Enable Delete Cookies (Scored)

Profile Applicability:

- Level 1

Description:

This feature deletes all cookies when using the Clear Private Data feature.

Rationale:

Deleting cookies via the Clear Private Data feature mitigates the risk of sensitive user data being compromised.

Audit:

Perform the following procedure:

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

```
privacy.item.cookies=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.item.cookies", "true")
```

6.12 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 mitigates the risk of unintentionally accessing malicious sites.

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")
```

6.13 Set Deferred Session Store Privacy Level (Scored)

Profile Applicability:

- Level 1

Description:

This feature decides what gets saved by Session Restore when intentionally quitting the browser.

Rationale:

Disabling the browser from saving items, such as forms, cookies, and scroll bar positions, minimizes the risk of user data and/or browser behavior being compromised.

Audit:

Perform the following procedure:

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

```
browser.sessionstore.privacy_level_deferred=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("browser.sessionstore.privacy_level_deferred", "2")
```

6.14 Set Session Store Privacy Level (Scored)

Profile Applicability:

- Level 1

Description:

This feature decides what gets saved by Session Restore when the browser unintentionally closes.

Rationale:

Disabling the browser from saving items, such as forms, cookies, and scroll bar positions, minimizes the risk of user data and/or browser behavior being compromised.

Audit:

Perform the following procedure:

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

```
browser.sessionstore.privacy_level=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("browser.sessionstore.privacy_level", "2")
```

6.16 Set "security-sensitive dialog boxes" to "2000" (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 disabled.

Rationale:

Setting the timer to 2000 mitigates the risk of data exposure from security-sensitive boxes left unattended.

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");
```

6.18 Set "security.checkloaduri" to "true" (Scored)

Profile Applicability:

- Level 1

Description:

This feature determines how to handle access across schemes

Rationale:

Setting this feature to true allows the browser to perform security checks and blocks access to/from unsecure items.

Audit:

Perform the following procedure:

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

```
security.checkloaduri=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.checkloaduri", "true");
```

6.19 Disable Clipboard Autocopy (Scored)

Profile Applicability:

- Level 2

Description:

This feature automatically copies all selected text in the browser to the clipboard.

Rationale:

Disabling this feature mitigates the risk that sensitive information will unknowingly be copied and potentially left available for untrusted sources.

Audit:

Perform the following procedure:

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

```
clipboard.autocopy=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("clipboard.autocopy", "false");
```

7 Extensions and Add-ons

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

7.1 Secure Application Plug-ins (Not 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 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.

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`

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`

7.2 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");
```

7.3 Set Missing Plugin URL (Scored)

Profile Applicability:

- Level 1

Description:

This feature determines the URL visited by Firefox to locate missing plugins for web content.

Rationale:

This feature mitigates the risk that a user will connect to a malicious site when searching for missing plugins for web content.

Audit:

Perform the following procedure:

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

```
pfs.datasource.url=https://pfs.mozilla.org/plugins/PluginFinderService.php?mime
type=%PLUGIN_MIMETYPE%&appID=%APP_ID%&appVersion=%APP_VERSION%&clientOS=%CLIENT
_OS%&chromeLocale=%CHROME_LOCALE%&appRelease=%APP_RELEASE%
```

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("pfs.datasource.url",
"https://pfs.mozilla.org/plugins/PluginFinderService.php?mimetype=%PLUGIN_MIMET
YPE%&appID=%APP_ID%&appVersion=%APP_VERSION%&clientOS=%CLIENT_OS%&chromeLocale=
%CHROME_LOCALE%&appRelease=%APP_RELEASE%");
```

7.4 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")
```

7.5 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")
```

7.7 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
```

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")
```

7.8 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");
```

7.9 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:

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 extension.blocklist.interval in the filter

3. Ensure the preferences listed are set to the values specified below:

```
extensions.block.list.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.block.list.interval", "86400");
```

8 Malware Settings

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

8.1 Enable Safe Browsing (Scored)

Profile Applicability:

- Level 1

Description:

This feature enables or disables the Safe Browsing function.

Rationale:

Enabling Safe Browsing helps to mitigate the risk of phishing or malware capabilities.

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");
```

8.2 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.

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");
```

8.3 Block Reported Web Forgeries (Scored)

Profile Applicability:

- Level 1

Description:

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

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.

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");
```

8.4 Enable Safe Browsing Warning (Scored)

Profile Applicability:

- Level 1

Description:

This feature enables a warning to be displayed when a phishy website is accessed.

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.

Audit:

Perform the following procedure:

1. Type `about:config` in the address bar

2. Type `browser.safebrowsing.warning.infoURL` in the filter
3. Ensure the preferences listed are set to the values specified below:

```
browser.safebrowsing.warning.infoURL=https://www.mozilla.org/%LOCALE%/firefox/p
hishing-protection/
```

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.warning.infoURL",
"https://www.mozilla.org/%LOCALE%/firefox/phishing-protection/");
```