the CENTER for INTERNET SECURITY

Security Configuration Benchmark For

Opera Browser

Version 1.1.0
November 15th, 2010

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

Terms of Use Agreement

Background.

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

No representations, warranties and covenants.

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

User agreements.

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

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

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

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

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

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

Grant of limited rights.

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

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

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

of this Agreed Terms of Use in its entirety.

Retention of intellectual property rights; limitations on distribution.

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

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

Special rules.

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

Choice of law; jurisdiction; venue.

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

Table of Contents

Overview

This document, *Security Configuration Benchmark for Opera*, provides prescriptive guidance for establishing a secure configuration posture for *Opera version 10.63* running on *Microsoft Windows Version 5.1 XP Professional: Service Pack 3 and Windows Vista (x86)*. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Consensus Guidance

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

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in to the CIS benchmark. If you are interested in participating in the consensus review process, please send us a note to 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 Opera Browser 10.63.

Acknowledgements

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

Authors
Waqas Nazir, *Digital Security, LLC.*

Contributors and Reviews
Blake Frantz, *Center for Internet Security*
Steffen Gransow
Remco Lanting
Chad Thunberg, *Leviathan Security Group*
Stephen Willis, *Qualys, Inc.*

Typographic Conventions

The following typographical conventions are used throughout this guide:

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

Configuration Levels

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

Level-I Benchmark Settings/Actions

Level-I Benchmark recommendations are intended to:

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

Level-II Benchmark Settings/Actions

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

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

Scoring Status

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

Scorable

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

Not Scorable

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

Recommendations

1. Opera Configurations

This section will provide guidance on secure configuration for Opera 10.51.

1.1 Pop-Up Blocker

This section will provide guidance on how to enable the Pop-Up blocker feature.

1.1.1 Enable Pop-up Blocker (Level I, Scorable)

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

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

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Click on the 'O' Opera button on the toolbar (top left corner)
3. Go to 'Settings'
4. Click on 'Preferences'
5. Click on 'General' tab
6. Select 'Block all pop-ups' in the 'Choose how you prefer to handle pop-ups' section

Audit:
Perform the following to determine if Opera is configured as recommended:

1. Close Opera browser and run the following command:

```
findstr /a:3 /isl "Ignore+Unrequested Popups=1" "%APPDATA%\Opera\Operaprefs.ini"
```

The following will result if the browser is configured as recommended:

```
Ignore Unrequested Popups=1
```

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

Default Value:
1

1.2 Data Storage

This section will provide guidance on how to secure user data used during browsing sessions.

1.2.1 Disallow Credential Storage (Level I, Scorable)

Description:
The Opera browser can remember both forms information and passwords. When you fill in a form and/or log in with a username and password, the browser will ask you if you would like to save the information. If you save the information, a yellow border will appear around the elements for which it has saved information the next time you visit the same page. It is recommended to disable credential storage.

Rationale:
If Opera or another application executing at an equal or higher security context is compromised, the confidentiality of authentication credentials will be at increased risk.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Click on the 'O' Opera button on the toolbar (top left corner)
3. Go to 'Settings'
4. Click on 'Preferences'
5. Click on the 'Forms' Tab
6. Deselect 'Enable Password Manager' and then click on 'Password Manager…' Button and 'Delete' any passwords listed in the dialog.
7. Click 'OK'

Audit:
Close Opera browser and run the following command:

```
findstr /a:3 /isl "Enable+ Wand=0" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Enable Wand=0
```

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

Default Value:
1

Additional References:

- Wand Feature: http://www.opera.com/products/desktop/wand/

1.2.2 Disallow Storage of Protected Information (Level I, Scorable)

Description:
Web pages which are password protected can be saved by Opera. It is recommended to disallow storage of password protected pages.

Rationale:
If Opera or another application executing at an equal or higher security context is compromised, the confidentiality of protected information will be at increased risk.

Remediation:
Use the following procedure:

1. Type 'opera:config' in the address bar
2. Type 'password' in the Quick Find Bar
3. Deselect 'Save Password Protected Pages'
4. Click 'Save'
5. Click 'Save' again on the confirmation dialog

Audit:
Close Opera browser and run the following command:

```
findstr /a:3 /isl "Save+Password+Protected Pages=0"
"%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Save Password Protected Pages=0
```

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

Default Value:
1

1.2.3 Disable Storage of Address Bar History (Level II, Scorable)

Description:
Opera can store the address of sites visited on the web. It is recommended to disable storage of browsing history in environments where security is paramount.

Rationale:
The address bar history may store sensitive URLs, such as those associated with cookieless web applications. Additionally, the address bar history details the user's browsing activity. If Opera or another application executing at an equal or higher security context is compromised, the confidentiality of browsing activity along with functionality exposed through cookieless session URLs is at increased risk.

Remediation:

Use the following procedure:

1. In the Opera Browser
2. Click on the 'O' Opera button on the toolbar (top left corner)
3. Go to 'Settings'
4. Click on 'Preferences'
5. Click on the 'Advanced' Tab
6. Click on 'History' from the left navigation menu.
7. Select '0' from 'Addresses' drop down
8. Click on 'Clear'
9. Click 'OK'

Audit:
Close Opera browser and run the following command:

```
findstr /a:3 /isl "Max+Global+History Lines=0" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Max Global History Lines=0
```

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

Default Value:
1000

References:

- http://msdn.microsoft.com/en-us/library/aa479314.aspx

1.2.4 Disable Storage of Page Data (Level II, Scorable)

Description:
Opera can store and index information from web pages visited during a browsing session. It is recommended to disable storage of page data.

Rationale:
If Opera or another application executing at an equal or higher security context is compromised, the confidentiality of browsing activity is at increased risk.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Click on the 'O' Opera button on the toolbar (top left corner)
3. Go to 'Settings'
4. Click on 'Preferences'
5. Click on the 'Advanced' Tab

6. Click on 'History' from the left navigation menu.
7. Deselect 'Remember content on visited pages'
8. Click 'OK'

Audit:
Close Opera browser and run the following command:

```
findstr /a:3 /isl "Visited+ Pages=0" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Visited Pages=0
```

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

Default Value:
1

1.3 Dynamic Content Options

This section will provide guidance on how to protect against malicious dynamic content.

1.3.1 Disable JavaScript's Ability to Hide the Address Bar (Level II, Scorable)

Description:
Address bar shows the location of the content when a page is loaded on the browser. It is recommended to disable JavaScript's ability to hide the address bar.

Rationale:
Some malicious websites can use JavaScript to hide the address bar so that a user cannot determine the location of the content. This will protect users from interacting with unknown web locations.

NOTE: If this configuration is not enabled, a user can always display a website's address by clicking the area below the title bar. Also, even when the address bar is hidden a minimized address bar with the domain of the content is loaded. The minimized address bar does not contain the complete location but just the domain name.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Click on the 'O' Opera button on the toolbar (top left corner)
3. Go to 'Settings'
4. Click on 'Preferences'
5. Click on the 'Advanced' Tab
6. Click on 'Content' from the left navigation menu.
7. Click on 'Javascript Options …' Button

8. Deselect 'Allow Script to hide Address Bar'
9. Click 'OK'
10. Click 'OK' to save

Audit:
Close Opera browser and run the following command:

```
findstr /a:3 /isl "Allow+script+to+hide address=0" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Allow script to hide address=0
```

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

Default Value:
1

1.3.2 Disable JavaScript's Ability to Change the Status Bar text (Level II, Scorable)

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. It is recommended to disable JavaScript's ability to change status bar text.

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. It is recommended to disallow JavaScript from changing the text on the Status Bar.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Click on the 'O' Opera button on the toolbar (top left corner)
3. Go to 'Settings'
4. Click on 'Preferences'
5. Click on the 'Advanced' Tab
6. Click on 'Content' from the left navigation menu.
7. Click on 'Javascript Options …' Button
8. Deselect 'Allow changing of Status field'
9. Click 'OK'
10. Click 'OK' to save

Audit:
Close Opera browser and run the following command:

```
findstr /a:3 /isl " Allow+script+to+change status=0"
"%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Allow script to change status=0
```

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

Default Value:
1

1.3.3 Disable Plug-ins (Level II, Scorable)

Description:
Plug-ins are used to allow third parties to extend the capabilities of the Opera browser. It is recommended to disable plug-ins in environments where security is paramount.

Rationale:
Some malicious websites can have active content to exploit vulnerabilities using Plug-ins. It is recommended as a defense-in-depth strategy to always disable unwanted features, such as Plug-ins.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Click on the 'O' Opera button on the toolbar (top left corner)
3. Go to 'Settings'
4. Click on 'Preferences'
5. Click on the 'Advanced' Tab
6. Click on 'Content' from the left navigation menu.
7. Deselect 'Enable Plug-ins' Button
8. Click 'OK' to save

Audit:
Close Opera browser and run the following command:

```
findstr /a:3 /isbp "plugins" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Plugins=0
```

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

Default Value:
1

1.4 Secure Cookies

This section will provide guidance on how to secure cookies used to track user sessions on the web.

1.4.1 Accept only 1st Party Cookies (Level II, Scorable)

Description:
1st party cookies are cookies that are set by the web site that appears in the Opera address bar. For example, if Opera visits www.example.org and the domain specified in a `Set-Cookie` header sent by the visited web server is example.org or a sub-domain of it, the cookie is considered a 1st party cookie. If Opera visits www.example.org and the domain specified in a `Set-Cookie` header sent by the visited web server is NOT example.org or a sub-domain of it, the cookie is considered a 3rd party cookie. Commonly, advertisement networks leverage 3rd party cookies to track browsing sessions across disparate web sites to build a profile for the user. It is recommended that Opera be configured to accept only 1st party cookies.

Rationale:
Configuring Opera to accept only 1st party cookies will limit the means by which an advertisement agency can build a browsing profile for the user.

Remediation:
Use the following procedure:

1. Click on 'Tools'
2. Click on the 'O' Opera button on the toolbar (top left corner)
3. Go to 'Settings'
4. Click on the 'Advanced' Tab
5. Click on 'Cookies' from the left navigation menu.
6. Select 'Accept only cookies from the site I visit'
7. Click 'OK'

Audit:
Close Opera browser and run the following command:

```
findstr /a:3 /isl "Enable+ Cookies=1" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Enable Cookies=1
```

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

Default Value:
14

1.5 Advanced Options

This section will provide guidance on some features of Opera to protect users.

1.5.1 Enable Fraud Protection by Opera (Level I, Scorable)

Description:
Opera uses a database of known malicious sites which may be phishing or malware spreading sites. This feature enables notification to a user when a user visits a malicious site. It is recommended to enable this protection.

Rationale:
This will provide users the ability to protect themselves from known reported malicious sites. This feature does not guarantee that all malicious sites will be flagged, but will provide some protection against malicious sites.

NOTE: With Opera Fraud Protection enabled, the domain name of Web sites a user visits is sent to Opera Software ASA's fraud protection server together with a hash of the domain name. HTTPS sites are checked via an encrypted channel, while IP addresses on the local intranet will never be checked.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Click on the 'O' Opera button on the toolbar (top left corner)
3. Go to 'Settings'
4. Click on 'Preferences'
5. Click on the 'Advanced' Tab
6. Click on 'Security' from the left navigation menu.
7. Select 'Enable Fraud and Malware Protection'
8. Click 'OK'

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "Enable+ Trust+ Rating" "%APPDATA%\Opera\operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Enable Trust Rating=1
```

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

Default Value:
1

1.6 Network Settings

This section will provide guidance on how to use strong encryption, and secure network settings.

1.6.1 Enable Strong Encryption Algorithm for SSL (Level I, Scorable)

Description:
Encryption Algorithms are used to protect data sent over the internet. The Opera browser supports a number of protocols and it is important to select strong algorithms. It is recommended to enable strong encryption for SSL.

Rationale:
Strong Encryption Algorithms will protect the data from being compromised when sent over the internet.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Click on the 'O' Opera button on the toolbar (top left corner)
3. Go to 'Settings'
4. Click on 'Preferences'
5. Click on the 'Advanced' Tab
6. Click on 'Security' from the left navigation menu.
7. Click on 'Security Protocols'
8. Select 'Enable SSL 3'
9. Click 'OK'

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "SSL" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Enable SSL v3=1
```

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

Default Value:
1

1.6.2 Disable TLS v1 (Level I, Scorable)

Description:
Encryption Algorithms are used to protect data sent over the internet. The Opera browser supports a number of protocols and it is important to select strong algorithms. It is recommended to disable TLS v1.0.

Rationale:
TLS v1 is known to be vulnerable to plain text attacks and it is recommended to disable TLS v1.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Click on the 'O' Opera button on the toolbar (top left corner)
3. Go to 'Settings'
4. Click on 'Preferences'
5. Click on the 'Advanced' Tab
6. Click on 'Security' from the left navigation menu.
7. Click on 'Security Protocols'
8. Deselect 'Enable TLS v 1'
9. Click 'OK'

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "TLS+ v1.0" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Enable TLS v1.0=0
```

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

Default Value:
1

1.6.3 Enable Strong Encryption Algorithm for TLS v1.1 (Level I, Scorable)

Description:
Encryption Algorithms are used to protect data sent over the internet. The Opera browser support a number of protocols and it is important to select strong algorithms. It is recommended to enable strong TLS v1.1.

Rationale:
Strong Encryption Algorithms will protect the data from being compromised when sent over the internet.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Click on the 'O' Opera button on the toolbar (top left corner)
3. Go to 'Settings'
4. Click on 'Preferences'

5. Click on the 'Advanced' Tab
6. Click on 'Security' from the left navigation menu.
7. Click on 'Security Protocols'
8. Select 'Enable TLS 1.1'
9. Click 'OK'

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "TLS+ v1.1" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Enable TLS v1.1=1
```

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

Default Value:
1

1.6.4 Enable Strong Encryption Algorithm for TLS v1.2 (Level I, Scorable)

Description:
Encryption Algorithms are used to protect data sent over the internet. The Opera browser supports a number of protocols and it is important to select strong algorithms. It is recommended to enable TLS v1.2.

Rationale:
Strong Encryption Algorithms will protect the data from being compromised when sent over the internet.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Type 'opera:config' in the address bar
3. Type 'TLS' in the search bar
4. Select 'Enable TLS v1.2'
5. Click 'Save'
6. Click 'OK' on the confirmation window

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "TLS+ v1.2" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Enable TLS v1.2=1
```

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

Default Value:
1

1.6.5 Enable Extended Validation for SSL Certificates (Level II, Scorable)

Description:
Strict EV Mode causes the Opera browser to enable the Extended Validation indicator if the content is loaded using an Extended Validation (EV) SSL Certificate. It is recommended that Strict EV Mode be enabled on high security environments.

Rationale:
Enabling this setting will provide additional assurance that the authenticity of all data rendered by the Opera browser has passed the Extended Validation process before Opera informs the user of the site's EV status.

NOTE: This setting will only provide the green Opera bar when all content on a page is signed using EV Extended Validation certificates.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Type 'opera:config' in the address bar
3. Type 'Strict EV' in the search bar
4. Select 'Strict EV Mode'
5. Click 'Save'
6. Click 'OK' on the confirmation window

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "Strict+ EV+ Mode" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Strict EV Mode=1
```

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

Default Value:
0

1.6.6 Validate Proxies (Level I, Not Scorable)

Description:
The Opera browser can be configured to connect to web resources via a proxy server. It is recommended that the list of proxy servers configured in the Opera browser be reviewed to ensure only trusted servers are listed.

Rationale:
The Opera browser reads an address and sends all traffic to those proxy addresses. If the proxy was maliciously set, it is possible to compromise a user's privacy and provide malicious content as well.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Click on 'Tools'
3. Click on 'Preferences'
4. Click on the 'Advanced' Tab
5. Click on 'Network' from the left navigation menu.
6. Click on 'Proxy Servers…'
7. Deselect all proxy servers that are not trusted.
8. Click 'OK'

Audit:
Use the following steps:

1. In the Opera Browser
2. Click on 'Tools'
3. Click on 'Preferences'
4. Click on the 'Advanced' Tab
5. Click on 'Network' from the left navigation menu.
6. Click on 'Proxy Servers…'
7. Ensure that no Proxy Servers are configured which an enterprise environment might not have configured .

NOTE: This setting can also be checked by viewing `operaprefs.ini` or `override.ini` for any configured proxies.

Default Value:
No proxies configured.

1.6.7 Enable OCSP Validation (Level I, Scorable)

Description:
The Online Certificate Status Protocol (OCSP) is used to obtain the revocation status of X.509 certificates. The OCSP Validate Certificates option determines if the Opera browser will leverage

certificate revocation information when validating a site's certificate. It is recommended that this option be enabled.

Rationale:
Enabling the OCSP Validate Certificates option will help ensure that the information contained in a certificate issued by a site is valid.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Type 'opera:config' in the address bar
3. Type 'OCSP' in the search bar
4. Select 'OCSP Validate Certificates'
5. Click 'Save'
6. Click 'OK' on the confirmation window

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "OCSP" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
OCSP Validate Certificates=1
```

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

Default Value:
1

1.6.8 Disable Opera Unite (Level I, Scorable)

Description:
Opera Unite allows applications loaded in the Opera browser to share information with other users over the Internet [2]. It is recommended that this feature be disabled.

Rationale:
Disabling Opera Unite will decrease the attack surface of the browser.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Type 'opera:config' in the address bar
3. Type 'Unite' in the search bar

4. Deselect ‘Enable Unite’
5. Click ‘Save’
6. Click ‘OK’ on the confirmation window

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "Unite" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Enable Unite=0
```

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

Default Value:
0

1.6.9 Disable Opera Link (Level II, Scorable)

Description:
Opera Sync allows storing personal preferences such as bookmarks online so that a user’s configuration can be applied to different machines. It is recommended that this feature be disabled.

Rationale:
Disabling Opera Sync will protect users from their personal preferences being stored and compromised in the event of an exploit.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Type ‘opera:config’ in the address bar
3. Type ‘Sync’ in the search bar
4. Deselect ‘Sync Enabled’
5. Click ‘Save’
6. Click ‘OK’ on the confirmation window

Audit:
Close Opera browser and run the following command:

```
findstr /a:3 /isl "Sync" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Sync Enabled=0
```

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

Default Value:
0

References:
http://link.opera.com

1.6.10 Disable Usage Statistics (Level II, Scorable)

Description:
The Opera browser can collect usage statistics and provide them to Opera Software ASA for the purpose of improving the Opera browser. It is recommended that this feature be disabled in high security environments

Rationale:
Disabling this feature will reduce the attack surface of the Opera browser and reduce the possibility of disclosing information related to browsing practices to third parties, such as Opera Software ASA.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Type 'opera:config' in the address bar
3. Type 'Usage' in the search bar
4. Deselect 'Enable Usage Statistics'
5. Click 'Save'
6. Click 'OK' on the confirmation window

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "Usage" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Enable Usage Statistics=0
```

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

Default Value:
1

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

Description:
Opera can be configured to warn the user before submitting form data over an insecure transport, such as HTTP. It is recommended that Opera be configured to warn the user in this scenario.

Rationale:
Warning the user before form data is sent over an insecure transport provides the user with the opportunity to approve or deny the request based on the data's security classification.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Type 'opera:config' in the address bar
3. Type 'Warn Insecure' in the search bar
4. Select 'Warn Insecure Form'
5. Click 'Save'
6. Click 'OK' on the confirmation window

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "Warn Insecure" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Warn Insecure Form=1
```

Repeat the audit steps above for each profile of interest, using an account with appropriate privileges for accessing profiles needed. The default value is 0.

1.6.12 Disable HTML Validation (Level II, Scorable)

Description:
The Opera browser can perform HTML validation on visited web sites. This feature is used to validate conformation to HTML standards. This can result in disclosure of data loaded on a web page. It is recommended to remove the URL used for this validation.

Rationale:
This will protect users from sending sensitive data to the website used for HTML validation.

NOTE: This configuration will affect developers who use this feature for conformation to HTML Standards.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Type 'opera:config' in the address bar
3. Type 'Validation' in the search bar
4. Remove the URL listed in 'Validation URL'
5. Click 'Save'
6. Click 'OK' on the confirmation window

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "Validation" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Validation URL=
```

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

Default Value:
http://validator.w3.org/check

1.6.13 Disable Tracking of Download History (Level II, Scorable)

Description:
The Opera browser can track and store download activity. It is recommended to disable tracking of download history.

Rationale:
This will protect users from their download history being compromised due to information leakage.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Type 'opera:config' in the address bar
3. Type 'Keep' in the search bar
4. Set 'Keep Entries Days' to '0'
5. Click 'Save'
6. Click 'OK' on the confirmation window

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "Keep" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Keep Entries Days=0
```

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

Default Value:
7

1.6.14 Disable Opera Turbo Mode (Level I, Scorable)

Description:
The Opera browser can load images, graphics, and websites faster by compressing them using Opera Software ASA's servers. It is recommended that Opera Turbo be disabled.

Rationale:
This will protect images, graphics, and websites from being disclosed to Opera Software ASA's servers.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Click on the 'O' Opera button on the toolbar (top left corner)
3. Go to 'Settings'
4. Go to 'Quick Preferences'
5. Deselect 'Enable Opera Turbo'

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "Turbo" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Use Web Turbo Mode=0
```

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

Default Value:
0

1.6.15 Disable Cross Domain Access (Level I, Scorable)

Description:
The Opera browser can access data loaded from domains other than the originating domain. It is recommended to disable cross domain access.

Rationale:
This will protect users from malicious websites accessing data and sessions from other domains.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Type 'opera:config' in the address bar
3. Type 'Cross' in the search bar
4. Deselect 'Allow Cross Domain Access'
5. Click 'Save'

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "Cross" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Allow Cross Domain Access=0
```

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

Default Value:
0

1.6.16 Disable IFrames (Level II, Scorable)

Description:
The Opera browser can load content from different locations on a single page using iframes. It is recommended to disable iframes.

Rationale:
Disabling iframes will reduce exposure to ClickJacking attacks.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Type 'opera:config' in the address bar
3. Type 'iframes' in the search bar
4. Deselect 'IFrames'
5. Click 'Save'
6. Click 'OK' on the confirmation window

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "IFrames" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
IFrames=0
```

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

Default Value:
1

References:

- http://www.owasp.org/index.php/Clickjacking

1.6.17 Ensure all Private Data is Removed (Level I, Scorable)

Description:
The Opera browser allows selecting which type of data is removed when clearing private data. It is recommended that all data be removed when clear private data feature is used.

Rationale:
This will ensure that no sensitive data is left stored by the browser.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Type 'opera:config' in the address bar
3. Type 'Flags' in the search bar
4. Set the value of 'CheckFlags' to '4095'
5. Click 'Save'
6. Click 'OK' on the confirmation window

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "CheckFlags" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
CheckFlags=4095
```

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

Default Value:
0

1.6.18 Only Allow Valid Certificates (Level II, Scorable)

Description:
The Opera browser can restrict the use of invalid certificates. It is recommended that the Opera browser be configured to disallow invalid certificates.

Rationale:
This will ensure that invalid certificates are not used to provide confidential information or breach its integrity.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Type 'opera:config' in the address bar
3. Type 'Minimum' in the search bar
4. Set the value of 'Minimum Security Level' to '1'
5. Click 'Save'
6. Click 'OK' on the confirmation window

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "Minimum" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Minimum Security Level=1
```

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

Default Value:
0

1.6.19 Enable Auto-Update (Level I, Scorable)

Description:
The Opera browser can automatically find and install updates when they are available. It is recommended that auto update be enabled for environments where formal patch management is not used.

Rationale:
This will ensure that all security patches are applied to the Opera browser which will reduce exposure to known vulnerabilities.

NOTE: Currently, the Opera browser uses https://autoupdate.opera.com for downloading updates. The location can be checked using `opera:config#AutoUpdate|AutoupdateServer` command .

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Type 'opera:config' in the address bar
3. Type 'Update Auto' in the search bar
4. Set the value of 'Level of Update Automation' to '2'
5. Click 'Save'
6. Click 'OK' on the confirmation window

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "Automation" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Level of Update Automation=2
```

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

Default Value:
1

1.6.20 Disable Messaging Client (Level II, Scorable)

Description:
The Opera browser has messaging clients such as email and chat. It is recommended to disable these messaging clients.

Rationale:
It is recommended to disable unused functionality to decrease the attack surface of the browser.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Type 'opera:config' in the address bar
3. Type 'E-mail' in the search bar
4. Deselect 'Show E-mail Client'
5. Click 'Save'
6. Click 'OK' on the confirmation window

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "E-mail" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Show E-mail=0
```

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

Default Value:
1

1.6.21 Disable Visited Website Tracking in Days (Level II, Scorable)

Description:
The Opera browser can color a link visited which can be used by malicious websites to enumerate history of visited links. A user's browsing activity can be stolen. It is recommended to disable tracking of visited links.

Rationale:
This will protect users from their browsing activity being disclosed.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Type 'opera:config' in the address bar
3. Type 'Expiry' in the search bar
4. Set 'Expiry' in the 'Link' section to '0'
5. Click 'Save'
6. Click 'OK' on the confirmation window

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "Expiry=0" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Expiry=0
```

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

Default Value:

10

1.6.22 Disable Visited Website Tracking in Hours (Level II, Scorable)

Description:
The Opera browser can color a visited link which can be used by malicious websites to enumerate history of visited links. It is recommended that visited website tracking be disabled.

Rationale:
This will protect users from having their browsing activity being disclosed.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Type 'opera:config' in the address bar
3. Type 'Expiry' in the search bar
4. Set 'Expiry (Hours)' in the 'Link' section to '0'
5. Click 'Save'
6. Click 'OK' on the confirmation window

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "Expiry (Hours)" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Expiry (Hours)=0
```

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

Default Value:
10

1.6.23 Disable Caching of SSL Pages (Level II, Scorable)

Description:
The Opera browser can cache SSL pages after exiting in order to render pages quickly. It is recommended to disable this feature to protect sensitive data from being compromised from the cache.

Rationale:
This will protect data loaded in the SSL sessions from being compromised out of the cache.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Type 'opera:config' in the address bar
3. Type 'cache https' in the search bar
4. Deselect 'Cache HTTPS After Sessions'
5. Click 'Save'
6. Click 'OK' on the confirmation window

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "Cache+ HTTPS+ After" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Cache HTTPS After Session=0
```

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

Default Value:
1

1.6.24 Disable Disk Caching of SSL Pages (Level II, Scorable)

Description:
The Opera browser can save SSL pages on the disk cache if more memory is required for the process. It is recommended to disable this feature to protect sensitive data from being written on the disk.

Rationale:
This will protect data loaded in the SSL sessions from being compromised out of the disk.

Remediation:
Use the following procedure:

1. In the Opera Browser
2. Type 'opera:config' in the address bar
3. Type 'cache https' in the search bar
4. Deselect 'Cache HTTPS'
5. Click 'Save'
6. Click 'OK' on the confirmation window

Audit:
Close the Opera browser and run the following command:

```
findstr /a:3 /isl "Cache+ HTTPS+ After" "%APPDATA%\Opera\Operaprefs.ini"
```

The following output will be displayed if the browser is configured as recommended:

```
Cache HTTPS=0
```

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

Default Value:
0

1.7 Informational Items

1.7.1 Opera Kiosk Mode (Informational, Not Scorable)

The Opera browser can be run in kiosk mode, which is a mode mainly suited for public information stands. Such stands are typically found in libraries, airports, bank offices, or shopping malls.

For details on running and configuring Opera to be run in Kiosk mode please visit:
http://www.opera.com/support/mastering/kiosk/

1.7.2 Opera Private Browsing (Informational, Not Scorable)

The Opera browser allows starting private browsing sessions in a new tab or a new window. The private browsing sessions are designed to remove all traces of the session from the computer. This is especially useful when using someone else's computer.

For details on using Private Browsing please visit:
http://help.opera.com/Windows/10.51/en/tabs.html#private

Appendix A: References

Resource	Location
1. Opera Configuration File Reference	http://www.opera.com/support/usingopera/operaini/
2. Opera Unite Configuration	http://www.opera.com/support/mastering/sysadmin/#configure-unite
3. Opera Sysadmin Configuration	http://www.opera.com/support/mastering/sysadmin/

Appendix B: Change History

Date	Version	Changes for this version
May 18th, 2010	1.0.0	Public Release
November 15th, 2010	1.1.0	• Updated to cover Opera 10.63 • Update 1.5.1 – "Fraud Protection" -> "Fraud and Malware Protection