the CENTER for
INTERNET SECURITY

Security Configuration Benchmark For

Apple Safari 4.0

Version 1.0.0
May 5th, 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 Apple Safari*, provides prescriptive guidance for establishing a secure configuration posture for Apple Safari 4.0 running on Microsoft Windows and Apple OSX. This benchmark was tested using Safari 4.0.5 on Microsoft Windows XP Professional: Service Pack 3 and Microsoft Windows Vista (x86) and Safari 4.0.3 on Apple OSX 10.5. 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 guide was created using a consensus review process comprised of volunteer and contract subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

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

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, users, and platform deployment personnel, who plan to develop, deploy, assess, use or secure solutions that incorporate Safari 4.0.

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
Mike de Libero*, MDE Development*
Blake Frantz*, Center for Internet Security*
Joe Wulf*, ProSync Technology Group, 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. Safari Configurations

This section provides guidance on the secure configuration for Safari 4.0.

Audit Steps for all Scorable configuration recommendations require that the Safari configuration file be converted from binary plist format to XML. Plist editor[1] and plutil.pl [2] can be used for this purpose. The Safari configuration file is stored at the following locations:

> (Windows) `%APPDATA%\Apple Computer\Preferences\com.apple.Safari.plist`
> (Apple OSX) `$HOME/Library/Preferences/com.apple.Safari.plist`

1.1 Security Settings

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

Description:
The Pop-Up Blocker is used to block pop-up windows which a website might open with or without any user interaction. Pop-ups can be used to open un-trusted malicious content. It is recommended that the Popup Blocker be enabled.

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

Remediation:
Perform the following within Safari:

Microsoft Windows:

1. Click on 'Edit' (Alt-E)
2. Select 'Block Pop-Up Windows' if not selected

Apple OSX:

1. Click on 'Safari'
2. Select 'Block Pop-Up Windows' if not selected

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

1. Open the `config.xml` file
2. Find the token `<key>WebKitJavaScriptCanOpenWindowsAutomatically</key>`
3. Ensure this token is immediately followed by `<false/>`

Repeat the above steps for other profiles which need to be accessed.

1.1.2 Validate Proxy Settings (Level I, Not Scorable)

Description:
Safari can be configured to send web related traffic through a proxy server. A proxy server acts as an intermediary between the web browser and web server. It is recommended that the list of proxy servers used by Safari be reviewed to ensure that only trusted servers are present in it.

Rationale:
Given a proxy server's position between the web browser and web server, it has the ability to read and alter all information that is not cryptographically protected. Given this, if an untrusted proxy server is configured in Safari, the information sent and received by Safari is at considerable risk.

Audit:
Perform the following within Safari:

Microsoft Windows:

1. Click on 'Edit' (Alt-E)
2. Click on 'Preferences'
3. Click on 'Advanced' Icon
4. Click on 'Change Settings …'
5. Click on 'LAN Settings'
6. Ensure that the proxy listed is trusted

Apple OSX:

1. Click on 'Safari'
2. Click on 'Preferences'
3. Click on 'Advanced' Icon
4. Click on 'Change Settings …'
5. Click on 'Proxies' tab
6. Ensure that the proxy listed is trusted

1.1.3 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 Safari address bar. For example, if Safari 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 Safari 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 Safari be configured to accept only 1st party cookies.

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

Remediation:
Perform the following within Safari:

Microsoft Windows:

1. Click on 'Edit' (Alt-E)
2. Click on 'Preferences'
3. Click on 'Security' Icon
4. In Accept Cookies Select 'Only from sites I visit'

Apple OSX:

1. Click on 'Safari'
2. Click on 'Preferences'
3. Click on 'Security' Icon
4. In Accept Cookies Select 'Only from sites I visit'

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

1. Open the `config.xml` file
2. Find the token `<key>WebKitCookieStorageAcceptPolicy</key>`
3. Ensure this token is immediately followed by `<integer>2</integer>` or nothing.

Repeat the above steps for other profiles which need to be accessed.

1.1.4 Prompt for Insecure Form Submissions (Level I, Scorable)

Description:
Safari can be configured to warn the user before submitting form data over an insecure transport, such as HTTP. It is recommended that Safari 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:
Perform the following within Safari:

Microsoft Windows:

1. Click on ‘Edit’ (Alt-E)
2. Click on ‘Preferences’
3. Click on ‘Security’ Icon
4. Check the option ‘Ask before sending a non-secure form to a secure website’

Apple OSX:

1. Click on ‘Safari’
2. Click on ‘Preferences’
3. Click on ‘Security’ Icon
4. Check the option ‘Ask before sending a non-secure form to a secure website’

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

1. Open the `config.xml` file
2. Find the token `<key>AskBeforeSubmittingInsecureForms</key>`
3. Ensure this token is immediately followed by `<true />` or nothing.

Repeat the above steps for other profiles which need to be accessed.

1.1.5 Disable Storage and Usage of Form Data (Level II, Scorable)

Description:
Safari can store the information typed in forms for later use on other websites. It is recommended that Safari be configured such that it does not store and auto-fill form contents.

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

Remediation:
Perform the following within Safari:

Microsoft Windows:

1. Click on ‘Edit’ (Alt-E)
2. Click on ‘Preferences’
3. Click on ‘AutoFill’ Button
4. Unselect ‘Other forms’
5. Click the “Edit” button and select “Remove All”

Apple OSX:

1. Click on ‘Safari’
2. Click on ‘Preferences’

3. Click on ‘AutoFill’ Button
4. Unselect ‘Other forms’
5. Click the “Edit” button and select “Remove All”

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

1. Open the `config.xml` file
2. Find the token `<key>AutoFillMiscellaneousForms</key>`
3. Ensure this token is immediately followed by `<false />` or nothing.

Repeat the above steps for other profiles which need to be accessed.

1.1.6 Disable Storage and Usage of Credentials (Level II, Scorable)

Description:
Safari can store and auto-fill authentication credentials used to access web sites visited by the user. It is recommended that Safari be configured such that it does not store and auto-fill authentication credentials.

Rationale:
If Safari or another application executing at an equal or higher security context is compromised, persisted authentication credentials are at increased risk.

Remediation:
Perform the following within Safari:

Microsoft Windows:

1. Click on ‘Edit’ (Alt-E)
2. Click on ‘Preferences’
3. Click on ‘AutoFill’ Button
4. Unselect ‘User names and passwords’
5. Click the “Edit” button and select “Remove All”

Apple OSX:

1. Click on ‘Safari’
2. Click on ‘Preferences’
3. Click on ‘AutoFill’ Button
4. Unselect ‘User names and passwords’
5. Click the “Edit” button and select “Remove All”

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

1. Open the `config.xml` file

2. Find the token `<key>AutoFillPasswords</key>`
3. Ensure this token is immediately followed by `<false />` or nothing.

Repeat the above steps for other profiles which need to be accessed.

1.1.7 Disable Storage and Usage of Address Book Card (Level II, Scorable)

Description:
Safari allows the user to enter personal and business contact information into an Address Book card. This information can then be used to populate web forms by pressing the AutoFill button. It is recommended that this capability be disabled in environments where security is paramount.

Rationale:
If Safari or another application executing at an equal or higher security context is compromised, persisted personal and business contact information are at increased risk.

Remediation:
Perform the following within Safari:

Microsoft Windows:

1. Click on 'Edit' (Alt-E)
2. Click on 'Preferences'
3. Click on 'AutoFill' Button
4. Unselect 'Using info from my Address Book card'
5. Click the "Edit" button and remove any existing contact information

Apple OSX:

1. Click on 'Safari'
2. Click on 'Preferences'
3. Click on 'AutoFill' Button
4. Unselect 'Using info from my Address Book card'
5. Click the "Edit" button and remove any existing contact information

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

1. Open the `config.xml` file
2. Find the token `<key>AutoFillFromAddressBook</key>`
3. Ensure this token is immediately followed by `<false />` or nothing.

Repeat the above steps for other profiles which need to be accessed.

1.1.8 Enable Safe Browsing (Level I, Scorable)

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

Rationale:
Users will be alerted about known malicious web sites, thus decreasing the probability of a user's browser or system being exploited by known malware or phishing site.

Remediation:
Perform the following within Safari:

Microsoft Windows:

1. Click on 'Edit' (Alt-E)
2. Click on 'Preferences'
3. Click on 'Security' Button
4. Select 'Warn when visiting a fraudulent website'

Apple OSX:

1. Click on 'Safari'
2. Click on 'Preferences'
3. Click on 'Security' Button
4. Select 'Warn when visiting a fraudulent website'

Audit:

Perform the following to determine if Safari is configured as recommended:

1. Open the config.xml file
2. Find the token `<key>WarnAboutFraudulentWebsites</key>`
3. Ensure this token is immediately followed by `<true />` or nothing.

Repeat the above steps for other profiles which need to be accessed.

1.1.9 Disable plug-ins (Level II, Scorable)

Description:
Plug-ins provides means for extending the capabilities and features native to Safari. It is recommended that Plug-ins be disabled on systems where security is paramount.

Rationale:
Plug-ins increase the remote attack surface of Safari. Additionally, some plug-ins do not undergo rigorous security testing and are therefore more likely to contain exploitable defects.

Remediation:
Perform the following within Safari:

Microsoft Windows:

1. Click on 'Edit' (Alt-E)
2. Click on 'Preferences'
3. Click on 'Security' Button
4. Unselect 'Enable plug-ins'

Apple OSX:

1. Click on 'Safari
2. Click on 'Preferences'
3. Click on 'Security' Button
4. Unselect 'Enable plug-ins'

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

1. Open the `config.xml` file
2. Find the token `<key>WebKitPluginsEnabled</key>`
3. Ensure this token is immediately followed by `<false/>` or nothing.

Repeat the above steps for other profiles which need to be accessed.

1.1.10 Disable Java (Level II, Scorable)

Description:
Java is used to load code in the local machine which has more access to the local operating systems resource and can be used as an attack vector.

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

Remediation:
Perform the following within Safari:

Microsoft Windows:

1. Click on 'Edit' (Alt-E)
2. Click on 'Preferences'
3. Click on 'Security' Button
4. Unselect 'Enable Java'

Apple OSX:

1. Click on 'Safari'
2. Click on 'Preferences'
3. Click on 'Security' Button
4. Unselect 'Enable Java'

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

1. Open the `config.xml` file
2. Find the token `<key>WebKitJavaEnabled</key>`
3. Ensure this token is immediately followed by `<false />` or nothing.

Repeat the above steps for other profiles which need to be accessed.

1.1.11 Disable JavaScript (Level II, Scorable)

Description:
JavaScript enables web site authors to create enhanced user interfaces. In support of this, JavaScript enables web sites to programmatically read and alter the document object model (DOM) for the rendered web site as well as instantiate various objects, such as asynchronous XML HTTP request (XHR) objects. It is recommended that JavaScript be disabled.

Rationale:
JavaScript continues to be an attack vector for exploiting vulnerabilities in the browser. Additionally, JavaScript is commonly leveraged by exploit authors to create a deterministic memory layout in support of increasing the reliability of exploits.

Remediation:
Perform the following within Safari:

Microsoft Windows:

1. Click on 'Edit' (Alt-E)
2. Click on 'Preferences'
3. Click on 'Security' Button
4. Unselect 'Enable JavaScript''

Apple OSX:

1. Click on 'Safari'
2. Click on 'Preferences'
3. Click on 'Security' Button
4. Unselect 'Enable JavaScript''

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

1. Open the `config.xml` file
2. Find the token `<key>WebKitJavaScriptEnabled</key>`
3. Ensure this token is immediately followed by `<false />` or nothing.

Repeat the above steps for other profiles which need to be accessed.

1.1.12 Use of Private Browsing (Informational, Not Scorable)

Description:
Safari provides private browsing for users who want to remove all traces of a session after a browsing session ends. This is particularly useful when using shared computers. Perform the following to enable private browsing:

Microsoft Windows:

1. Click on 'Edit' (Alt-E)
2. Click on 'Private Browsing'

Apple OSX:

1. Click on 'Safari'
2. Click on 'Private Browsing'

For more information on Private Browsing, see
http://www.apple.com/pro/tips/privacy_safari.html

Appendix A: References

Resource	Location
1. pList Editor	http://www.topshareware.com/plist-Editor-for-Windows-transfer-67471.htm
2. plutil.pl	http://scw.us/iPhone/plutil/

Appendix B: Change History

Date	Version	Changes for this version
May 5th, 2010	1.0.0	Public Release