CIS Google Chrome Benchmark

Current release

Authors	
Owner	
Version Number	2.0.0
Approved by	
Release Date	2019-05-17
Classification	public
Document ID	CIS_Google_Chrome

Document History

Version	Author	Date	Description
2.0.0		2019-05-17	accepted

Change Log in the Current Version

Table of Contents

Notice

This content has been produced from an import of the

CIS Google Chrome Baseline (v2.0)

SCAP datastream into the Scapolite format.

Please refer to the slide set about Scapolite that has been presented at NIST’s SCAP v2 workshop for more information about Scapolite.

The machine-readable information on how to implement the settings is *not* part of the original CIS Benchmark; the information has been added using the mechanisms described in the slide set about automating implementation that has been presented at NIST’s SCAP v2 workshop.

Copyright holder for the contents of the CIS Google Chrome Baseline (v2.0), is CIS, please refer to the CIS Website for information about CIS Benchmarks and access to the authoritative versions of the benchmarks.

This project merely uses the CIS Benchmark as an example of how SCAP content can be expressed and enriched in Scapolite. We are grateful to CIS for allowing us to publish this transformed version of their content!

For feedback/questions/discussion please use the mailing list

https://list.nist.gov/scap-dev-authoring

BACKGROUND. The Center for Internet Security (“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, OR 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 the Products or the Recommendations. 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: 1. No network, system, device, hardware, software, or component can be made fully secure; 2. We are using the Products and the Recommendations solely at our own risk; 3. 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; 4. 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; 5. Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades, or bug fixes; or to notify us of the need for any such corrections, updates, upgrades, or bug fixes; and 6. 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: 1. 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; 2. 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. BY USING THE PRODUCTS I(WE) ACKNOWLEDGE THAT WE HAVE READ THESE AGREED TERMS OF USE IN THEIR ENTIRETY, UNDERSTAND THEM, AND I(WE) AGREE TO BE BOUND BY THEM IN ALL RESPECTS.

Introduction

Objectives

This document provides prescriptive guidance for establishing a secure configuration posture for Google Chrome Browser. This guide was tested against Google Chrome v75. 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.

Enforced Defaults

This section contains recommendations that are configured by default when you install Google Chrome. Enforcing these settings at an enterprise level can prevent these settings from changing to a less secure option.

Remote access

This section contains recommendations related to Remote Access that are configured by default when you install Google Chrome. Enforcing these settings at an enterprise level can prevent these settings from changing to a less secure option.

R1.1.1

(L1) Ensure ‘Enable curtaining of remote access hosts’ is set to ‘Disabled’

(L1) Ensure ‘Enable curtaining of remote access hosts’ is set to ‘Disabled’

Rationale

If a remote session is in progress the user physically present at the host machine shall be able to see what a remote user is doing.

Description

Chrome allows controls to prevent someone physically present at the host machine from seeing what a user is doing while a remote connection is in progress.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Configure remote access
options\Enable curtaining of remote access hosts
```

Impact:

If this setting is disabled, host’s physical input and output devices are enabled while a remote connection is in progress.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Configure
  remote access options\Enable curtaining of remote access hosts
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: RemoteAccessHostRequireCurtain
action: DWORD:0
```

R1.1.2

(L1) Ensure ‘Allow gnubby authentication for remote access hosts’ is set to ‘Disabled’.

(L1) Ensure ‘Allow gnubby authentication for remote access hosts’ is set to ‘Disabled’.

Rationale

Proxying shall not be used to circumvent firewall restrictions.

Description

Google Chrome offers to proxy gnubby authentication requests (U2F) across a remote host connection.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

`Computer Configuration\Administrative Templates\Google\Google Chrome\Configure remote access options\Allow gnubby authentication for remote access hosts`

Impact:

If this setting is disabled, gnubby authentication requests will not be proxied.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Configure
  remote access options\Allow gnubby authentication for remote access hosts
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: RemoteAccessHostAllowGnubbyAuth
action: DWORD:0
```

R1.1.3

(L1) Ensure ‘Allow remote users to interact with elevated windows in remote assistance sessions’ is set to ‘Disabled’

(L1) Ensure ‘Allow remote users to interact with elevated windows in remote assistance sessions’ is set to ‘Disabled’

Rationale

Remote users shall not be able to escalate privileges.

Description

Google Chrome offers to run the remote assistance host in a process with uiAccess permissions. This allows remote users to interact with elevated windows on the local user’s desktop.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

`Computer Configuration\Administrative Templates\Google\Google Chrome\Configure remote access options\Allow remote users to interact with elevated windows in remote assistance sessions`

Impact:

If this setting is disabled, the remote assistance host will run in the user’s context. Furthermore, remote users cannot interact with elevated windows on the desktop.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Configure
  remote access options\Allow remote users to interact with elevated windows in remote
  assistance sessions
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: RemoteAccessHostAllowUiAccessForRemoteAssistance
action: DWORD:0
```

R1.2

(L1) Ensure ‘Continue running background apps when Google Chrome is closed’ is set to ‘Disabled’

(L1) Ensure ‘Continue running background apps when Google Chrome is closed’ is set to ‘Disabled’

Rationale

If this setting is enabled, vulnerable or malicious plugins, apps and processes can continue running even after Chrome has closed.

Description

Chrome allows for processes started while the browser is open to remain running once the browser has been closed. It also allows for background apps and the current browsing session to remain active after the browser has been closed.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

`Computer Configuration\Administrative Templates\Google\Google Chrome\Continue running background apps when Google Chrome is closed`

Impact:

If this policy is set to Disabled, background mode is disabled and cannot be controlled by the user in the browser settings.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Continue
  running background apps when Google Chrome is closed
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: BackgroundModeEnabled
action: DWORD:0
```

R1.3

(L1) Ensure ‘Ask where to save each file before downloading’ is set to ‘Enabled’

(L1) Ensure ‘Ask where to save each file before downloading’ is set to ‘Enabled’

Rationale

Users shall be prevented from the drive-by-downloads threat.

Description

Google Chrome offers to download files automatically to the default download directory without prompting.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Ask where to save each file
before downloading
```

Impact:

If this setting is enabled, users are always asked where to save each file before downloading.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Ask
  where to save each file before downloading
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: PromptForDownloadLocation
action: DWORD:1
```

R1.4

(L1) Ensure ‘Disable saving browser history’ is set to ‘Disabled’

(L1) Ensure ‘Disable saving browser history’ is set to ‘Disabled’

Rationale

Browser history shall be saved as it may contain indicators of compromise.

Description

Google Chrome allows to save the browser history.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Disable saving browser history`

Impact:

All user browser history will be saved.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Disable
  saving browser history
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: SavingBrowserHistoryDisabled
action: DWORD:0
```

R1.5

(L1) Ensure ‘Enable HTTP/0.9 support on non-default ports’ is set to ‘Disabled’

(L1) Ensure ‘Enable HTTP/0.9 support on non-default ports’ is set to ‘Disabled’

Rationale

DNS rebinding attacks can be mounted against non-HTTP services to steal their responses cross-protocol.

Description

Non-HTTP services’ responses may be read via XHR as their response streams will be interpreted by Chrome as HTTP/0.9. This setting allows to enable HTTP/0.9 on ports other than 80 for HTTP and 443 for HTTPS.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Enable HTTP/0.9 support on non-default ports`

Impact:

If this setting is disabled, HTTP/0.9 will be disabled on non-default ports 80/443.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
  HTTP/0.9 support on non-default ports
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: Http09OnNonDefaultPortsEnabled
action: DWORD:0
```

R1.6

(L1) Ensure ‘Enable component updates in Google Chrome’ is set to ‘Enabled’

(L1) Ensure ‘Enable component updates in Google Chrome’ is set to ‘Enabled’

Rationale

Google Chrome Updater shall be used to keep the components bundled to Chrome up-to-date.

Description

Google Chrome’s Component Updater updates several components of Google Chrome (like the Adobe Flash Player, Widevine DRM, Chrome updater recovery component) on a regular basis.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Enable component updates in Google Chrome`

Impact:

Google Chrome Updater keeps the components bundled to Chrome up-to-date.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
  component updates in Google Chrome
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: ComponentUpdatesEnabled
action: DWORD:1
```

R1.7

(L1) Ensure ‘Enable deprecated web platform features for a limited time’ is set to ‘Disabled’

(L1) Ensure ‘Enable deprecated web platform features for a limited time’ is set to ‘Disabled’

Rationale

Deprecated web platform features shall no longer be used.

Description

Google Chrome offers the ability to re-enable specific deprecated web platform features for a defined period of time.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Enable deprecated web platform features for a limited time`

Impact:

If this setting is disabled, deprecated web platform features are no longer being reactivated.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
  deprecated web platform features for a limited time
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome\EnableDeprecatedWebPlatformFeatures
value_name: '*'
action: CLEAR
```

R1.8

(L1) Ensure ‘Enable third party software injection blocking’ is set to ‘Enabled’

(L1) Ensure ‘Enable third party software injection blocking’ is set to ‘Enabled’

Rationale

Third party software shall not be able to inject executable code into Chrome’s processes.

Description

Google Chrome allows to prevented third party software from injecting executable code into Chrome’s processes.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Enable third party software injection blocking`

Impact:

Third party software will be prevented from injecting executable code into Chrome’s processes.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
  third party software injection blocking
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: ThirdPartyBlockingEnabled
action: DWORD:1
```

R1.9

(L1) Ensure ‘Extend Flash content setting to all content’ is set to ‘Disabled’

(L1) Ensure ‘Extend Flash content setting to all content’ is set to ‘Disabled’

Rationale

Cross-domain Flash plugins or “hidden” flash content may be malicious and therefore shall be prevented from being displayed.

Description

Controls if all Flash content embedded on websites that have been set to allow Flash in content settings - either by the user or by enterprise policy - will be run, including content from other origins or small content.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Extend Flash content setting to all content`

Impact:

Flash content from other origins or small content might be blocked.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Extend
  Flash content setting to all content
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: RunAllFlashInAllowMode
action: DWORD:0
```

R1.10

(L1) Ensure ‘Suppress the unsupported OS warning’ is set to ‘Disabled’

(L1) Ensure ‘Suppress the unsupported OS warning’ is set to ‘Disabled’

Rationale

The user shall be informed if the used software is no longer supported.

Description

Google Chrome will show a warning that appears when Google Chrome is running on a computer or operating system that is no longer supported.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Suppress the unsupported OS warning`

Impact:

Unsupported warnings will not be suppressed.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Suppress
  the unsupported OS warning
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: SuppressUnsupportedOSWarning
action: DWORD:0
```

R1.11

(L1) Ensure ‘Whether online OCSP/CRL checks are performed’ is set to ‘Disabled’

(L1) Ensure ‘Whether online OCSP/CRL checks are performed’ is set to ‘Disabled’

Rationale

An attacker may block OCSP traffic and cause revocation checks to pass in order to cause usage of soft-fail behavior. Furthermore, the browser may leak what website is being accessed and who accesses it to CA servers.

Description

Google Chrome offers to reactivate soft-fail, online revocation checks although they provide no effective security benefit.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Whether online OCSP/CRL checks are performed`

Impact:

If this setting is disabled, unsecure online OCSP/CRL checks are no longer performed.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Whether
  online OCSP/CRL checks are performed
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: EnableOnlineRevocationChecks
action: DWORD:0
```

R1.12

(L1) Ensure ‘Allow WebDriver to Override Incompatible Policies’ is set to ‘Disabled’

(L1) Ensure ‘Allow WebDriver to Override Incompatible Policies’ is set to ‘Disabled’

Rationale

Settings of policies shall not be circumvented by any features.

Description

The WebDriver feature may override policies which can interfere with its operation. At time of writing this may affect the policies ‘Enable Site Isolation for every site’ and ‘Enable Site Isolation for specified origins’.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Allow WebDriver to Override Incompatible Policies`

Impact:

WebDriver will not be allowed to override incompatible policies.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Allow
  WebDriver to Override Incompatible Policies
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: WebDriverOverridesIncompatiblePolicies
action: DWORD:0
```

R1.13

(L1) Ensure ‘Control SafeSites adult content filtering’ is set to ‘Enabled’ with value ‘Do not filter sites for adult content’ specified

(L1) Ensure ‘Control SafeSites adult content filtering’ is set to ‘Enabled’ with value ‘Do not filter sites for adult content’ specified

Rationale

Using Googles Safe Search API may leak information which is typed/pasted by mistake into the omnibox, e.g. passwords, internal webservices, folder structures, etc.

Description

Google Chrome allows to use the Google Safe Search API to classify URLs as pornographic or not.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with value `Do not filter sites for adult content` specified:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Control SafeSites adult content filtering.`

Impact:

Sites will not be filtered.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Control
  SafeSites adult content filtering.
value: Do not filter sites for adult content
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: SafeSitesFilterBehavior
action: DWORD:0
```

R1.14

(L1) Ensure ‘Origins or hostname patterns for which restrictions on insecure origins should not apply’ is set to ‘Disabled’

(L1) Ensure ‘Origins or hostname patterns for which restrictions on insecure origins should not apply’ is set to ‘Disabled’

Rationale

Insecure contexts shall always be labeled as insecure.

Description

Google Chrome allows to specify a list of origins (URLs) or hostname patterns (such as “*.example.com”) for which security restrictions on insecure origins will not apply and are prevented from being labeled as “Not Secure” in the omnibox.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Origins or hostname patterns for which restrictions on insecure origins should not apply`

Impact:

Insecure contexts are labeled as insecure.

01 Machine readable information

Windows GPO Setting

```
ui_path: "Computer Configuration\\Administrative Templates\\Google\\Google Chrome\\\
  Origins or hostname patterns for which restrictions on\ninsecure origins should\
  \ not apply"
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome\OverrideSecurityRestrictionsOnInsecureOrigin
value_name: '*'
action: CLEAR
```

R1.15

(L1) Ensure ‘Disable Certificate Transparency enforcement for a list of Legacy Certificate Authorities’ is set to ‘Disabled’

(L1) Ensure ‘Disable Certificate Transparency enforcement for a list of Legacy Certificate Authorities’ is set to ‘Disabled’

Rationale

Legacy Certificate Authorities shall follow the Certificate Transparency policy.

Description

Google Chrome allows to disable the enforcing of Certificate Transparency requirements for a list of Legacy Certificate Authorities.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Disable Certificate Transparency enforcement for a list of Legacy Certificate Authorities`

Impact:

If this setting is disabled, certificates not properly publicly disclosed as required by Certificate Transparency are untrusted.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Disable
  Certificate Transparency enforcement for a list of Legacy Certificate Authorities
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome\CertificateTransparencyEnforcementDisabledForLegacyCas
value_name: '*'
action: CLEAR
```

R1.16

(L1) Ensure ‘Disable Certificate Transparency enforcement for a list of URLs’ is set to ‘Disabled’

(L1) Ensure ‘Disable Certificate Transparency enforcement for a list of URLs’ is set to ‘Disabled’

Rationale

Certificates that are required to be disclosed via Certificate Transparency shall be treated for all URLs as untrusted if they are not disclosed according to the Certificate Transparency policy.

Description

Google Chrome allows to specify URLs/hostnames for which Certificate Transparency will not be enforced.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Disable Certificate Transparency enforcement for a list of URLs`

Impact:

If this setting is disabled, no URLs are excluded from Certificate Transparency requirements.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Disable
  Certificate Transparency enforcement for a list of URLs
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome\CertificateTransparencyEnforcementDisabledForUrls
value_name: '*'
action: CLEAR
```

R1.17

(L1) Ensure ‘Disable Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes’ is set to ‘Disabled’

(L1) Ensure ‘Disable Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes’ is set to ‘Disabled’

Rationale

Certificate Transparency requirements shall be enforced for all certificates.

Description

Google Chrome allows to exclude certificates by their subjectPublicKeyInfo hashes from enforcing Certificate Transparency requirements.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Disable Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes`

Impact:

If this setting is disabled, no certificates are excluded from Certificate Transparency requirements.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Disable
  Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome\CertificateTransparencyEnforcementDisabledForCas
value_name: '*'
action: CLEAR
```

Attack Surface Reduction

This section contains recommendations that help reduce the overall attack surface. Organizations should review these settings and any potential impacts to ensure they make sense within the environment since they restrict some browser functionality.

R2.1

(L1) Ensure ‘Default Flash Setting’ is set to ‘Enabled’ (Click to Play)

(L1) Ensure ‘Default Flash Setting’ is set to ‘Enabled’ (Click to Play)

Rationale

Malicious plugins can cause browser instability and erratic behavior so setting the value to ‘Click to play’ will allow a user to only run necessary plugins.

Description

Allows you to set whether websites are allowed to automatically run plugins. Automatically running plugins can be either allowed for all websites or denied for all websites.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with `Click to play` selected from the drop down.

`Computer Configuration\Administrative Templates\Google\Google Chrome\Content Settings\Default Flash Setting`

Impact:

If this setting is enabled, users must click plugins to allow their execution

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Content
  Settings\Default Flash setting
value: Click to play
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: DefaultPluginsSetting
action: DWORD:3
```

R2.2

(L2) Ensure ‘Default notification setting’ is set to ‘Enabled’ with ‘Do not allow any site to show desktop notifications’

(L2) Ensure ‘Default notification setting’ is set to ‘Enabled’ with ‘Do not allow any site to show desktop notifications’

Rationale

If the website operator decides to send messages unencrypted Google’s servers may process it as plain text. Furthermore, potentially compromised or faked notifications might trick users into clicking on a malicious link.

Description

Google Chrome offers websites to display desktop notifications. These are push messages which are sent from the website operator through Google infrastructure to Chrome.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with `Do not allow any site to show desktop notifications` selected from the drop down:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Content Settings\Default notification setting`

Impact:

If this setting is enabled and set to `Do not allow any site to show desktop notifications`, notifications will not be displayed for any sites and the user will not be asked.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Content
  Settings\Default notification setting
value: Do not allow any site to show desktop notifications
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: DefaultNotificationsSetting
action: DWORD:2
```

R2.3

(L2) Ensure ‘Control use of the Web Bluetooth API’ is set to ‘Enabled’ with ‘Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API’

(L2) Ensure ‘Control use of the Web Bluetooth API’ is set to ‘Enabled’ with ‘Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API’

Rationale

A malicious website could exploit a vulnerable Bluetooth device.

Description

Google Chrome offers a API which allows the access to nearby Bluetooth devices from the browser with users consent.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with `Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API` selected from the drop down:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Content Settings\Control use of the Web Bluetooth API`

Impact:

If this setting is enabled and set to `Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API`, websites no longer can access nearby Bluetooth device via the API and the user will never be asked.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Content
  Settings\Control use of the Web Bluetooth API
value: Do not allow any site to request access to Bluetooth devices via the Web Bluetooth
  API
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: DefaultWebBluetoothGuardSetting
action: DWORD:2
```

R2.4

(L2) Ensure ‘Control use of the WebUSB API’ is set to ‘Enabled’ with ‘Do not allow any site to request access to USB devices via the WebUSB API’

(L2) Ensure ‘Control use of the WebUSB API’ is set to ‘Enabled’ with ‘Do not allow any site to request access to USB devices via the WebUSB API’

Rationale

WebUSB is opening the doors for sophisticated phishing attacks that could bypass hardware-based two-factor authentication devices (e.g. Yubikey devices).

Description

Google Chrome offers a API which allows the access to connected USB devices from the browser.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with `Do not allow any site to request access to USB devices via the WebUSB API` selected from the drop down:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Content Settings\Control use of the WebUSB API`

Impact:

If this setting is enabled and set to `Do not allow any site to request access to USB devices via the WebUSB API`, websites can no longer access connected USB devices via the API which could also prevent 2FA USB devices from working properly.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Content
  Settings\Control use of the WebUSB API
value: Do not allow any site to request access to USB devices via the WebUSB API
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: DefaultWebUsbGuardSetting
action: DWORD:2
```

R2.5

(L1) Ensure ‘Configure extension installation blacklist’ is set to ‘Enabled’ (“*” for all extensions)

(L1) Ensure ‘Configure extension installation blacklist’ is set to ‘Enabled’ (“*” for all extensions)

Rationale

This can be used to block extensions that could potentially allow remote control of the system through the browser. If there are extensions needed for securing the browser or for enterprise use these can be enabled by configuring either the policy `Configure extension installation whitelist` or the policy `Extension management settings`.

Description

Enabling this setting allows you to specify which extensions the users can NOT install. Extensions already installed will be removed if blacklisted.

NOTE: Chrome does offer a more granular permission based configuration called `Extension management settings` if blacklisting all extensions is too aggressive, which allows an organization to drill down to the exact permissions that they want to lock down. The extensions management settings requires more coordination and effort to understand what the security requirements are to block site and device permissions globally as well as more IT management to deploy the policy, the benefit would allow access to more extensions to their end-users. See link in reference section

NOTE 2: If Chrome Cleanup is Disabled, users my want to configure the extension blacklist instead of using the Extension Management option. Chrome Cleanup can help protect against malicious extensions when paired with the Extension Management policy.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with value `*` specified.

`Computer Configuration\Administrative Templates\Google\Google Chrome\Extensions\Configure Extension Installation Blacklist`

Impact:

Any installed extension will be removed unless it is specified on the extension whitelist, if an organization is using any approved password managers ensure that the extension is added to the whitelist.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Extensions\Configure
  extension installation blacklist
value:
- '*'
```

Compound automation

Carry out the following automations:

- **Windows Registry Setting**

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome\ExtensionInstallBlacklist
value_name: '*'
action: DELETEALLVALUES
```

- **Windows Registry Setting**

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome\ExtensionInstallBlacklist
value_name: '1'
action: SZ:*
```

R2.6

(L1) Ensure ‘Configure allowed app/extension types’ is set to ‘Enabled’ with the values ‘extension’, ‘hosted_app’, ‘platform_app’, ‘theme’ specified

(L1) Ensure ‘Configure allowed app/extension types’ is set to ‘Enabled’ with the values ‘extension’, ‘hosted_app’, ‘platform_app’, ‘theme’ specified

Rationale

App or extension types that could be misused or are deprecated shall no longer be installed.

Description

Enabling this setting allows you to specify which app/extensions types are allowed.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with values `extension`, `hosted_app`, `platform_app`, `theme` specified:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Extensions\Configure allowed app/extension types`

Impact:

Extensions already installed will be removed if it’s type is blacklisted and the extension itself is not whitelisted.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Extensions\Configure
  allowed app/extension types
value:
- platform_app
- extension
- hosted_app
- theme
```

Compound automation

Carry out the following automations:

- **Windows Registry Setting**

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome\ExtensionAllowedTypes
value_name: '*'
action: DELETEALLVALUES
```

- **Windows Registry Setting**

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome\ExtensionAllowedTypes
value_name: '1'
action: SZ:platform_app
```

- **Windows Registry Setting**

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome\ExtensionAllowedTypes
value_name: '2'
action: SZ:extension
```

- **Windows Registry Setting**

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome\ExtensionAllowedTypes
value_name: '3'
action: SZ:hosted_app
```

- **Windows Registry Setting**

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome\ExtensionAllowedTypes
value_name: '4'
action: SZ:theme
```

R2.7

(L2) Ensure ‘Configure native messaging blacklist’ is set to ‘Enabled’ (“*” for all messaging applications)

(L2) Ensure ‘Configure native messaging blacklist’ is set to ‘Enabled’ (“*” for all messaging applications)

Rationale

For consistency with Plugin and Extension policies, native messaging should be blacklisted by default, requiring explicit administrative approval of applications for whitelisting. Examples of applications that use native messaging is the 1Password password manager.

Description

Allows you to specify which native messaging hosts that should not be loaded.

Note: This needs to be handled carefully. If an extension is enabled, yet can’t communicate with its backend code, it could behave in strange ways which results in helpdesk tickets + support load.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with value `*` specified.

`Computer Configuration\Administrative Templates\Google\Google Chrome\Native Messaging\Configure native messaging blacklist`

Impact:

A blacklist value of ‘*’ means all native messaging hosts are blacklisted unless they are explicitly listed in the whitelist.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Native
  Messaging\Configure native messaging blacklist
value:
- '*'
```

Compound automation

Carry out the following automations:

- **Windows Registry Setting**

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome\NativeMessagingBlacklist
value_name: '*'
action: DELETEALLVALUES
```

- **Windows Registry Setting**

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome\NativeMessagingBlacklist
value_name: '1'
action: SZ:*
```

R2.8

(L1) Ensure ‘Enable saving passwords to the password manager’ is Configured

(L1) Ensure ‘Enable saving passwords to the password manager’ is Configured

Rationale

The Google Chrome password manager is ON by default and each organization should review and determine if they want to allow users to store passwords in the Browser. If another solution is used instead of the built in Chrome option then an organization should configure the setting to Disabled.

Description

Google Chrome has a built in password manager to store passwords for users. Chrome will use local authentication to allow users to gain access to these passwords.

NOTE: If you choose to Enable this setting please review `Disable synchronization of data with Google` and ensure this setting is configured to meet organizational requirements.

01 Implementation Example

To establish the recommended configuration via Group Policy, configure the following setting to meet organizational requirements:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Password manager\Enable the password manager`

Impact:

If this settings is disabled, users cannot save new passwords but they may still use passwords that have been saved previously.

If this settings is enabled or not configured, users can save passwords.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Password
  manager\Enable saving passwords to the password manager
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: PasswordManagerEnabled
action: DWORD:0
```

R2.9

(L1) Ensure ‘Supported authentication schemes’ is set to ‘Enabled’ (ntlm, negotiate)

(L1) Ensure ‘Supported authentication schemes’ is set to ‘Enabled’ (ntlm, negotiate)

Rationale

Possible values are ‘basic’, ‘digest’, ‘ntlm’ and ‘negotiate’. Basic and Digest authentication do not provide sufficient security and can lead to submission of users password in plaintext or minimal protection.

Description

Specifies which HTTP authentication schemes are supported by Google Chrome.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled:(ntlm, negotiate)`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Policies for HTTP
Authentication\Supported authentication schemes
```

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Policies
  for HTTP authentication\Supported authentication schemes
value:
- Enabled:(ntlm, negotiate)
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: AuthSchemes
action: SZ:['Enabled:(ntlm, negotiate)']
```

R2.10

(L1) Ensure ‘Choose how to specify proxy server settings’ is not set to ‘Enabled’ with ‘Auto detect proxy settings’

(L1) Ensure ‘Choose how to specify proxy server settings’ is not set to ‘Enabled’ with ‘Auto detect proxy settings’

Rationale

Attackers may abuse the WPAD auto-config functionality to supply computers with a PAC file that specifies a rogue web proxy under their control.

Description

Google Chrome offers the functionality to configure the proxy settings by automatic discovery using WPAD (Web Proxy Auto-Discovery Protocol).

01 Implementation Example

To establish the recommended configuration via Group Policy, make sure the following UI path is not set to ‘Enabled’ with ‘Auto detect proxy settings’:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Proxy server\Choose how to specify proxy server settings
```

Impact:

If the policy is enabled, the proxy configuration will no longer be discovered using WPAD.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Proxy
  server\Choose how to specify proxy server settings
value: Auto detect proxy settings
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: ProxyMode
action: SZ:auto_detect
```

R2.11

(L1) Ensure ‘Allow running plugins that are outdated’ is set to ‘Disabled’

(L1) Ensure ‘Allow running plugins that are outdated’ is set to ‘Disabled’

Rationale

Running the most up-to-date version of a plugin can reduce the possibility of running a plugin that contains an exploit or security hole.

Description

Chrome enables the use of outdated plugins. By disabling this feature Chrome will not prompt the user to use an outdated plugin.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

`Computer Configuration\Administrative Templates\Google\Google Chrome\Allow running plugins that are outdated`

Impact:

If you disable this setting, outdated plugins will not be used and users will not be asked for permission to run them.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Allow
  running plugins that are outdated
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: AllowOutdatedPlugins
action: DWORD:0
```

R2.12

(L1) Ensure ‘Enable Google Cloud Print Proxy’ is set to ‘Disabled’

(L1) Ensure ‘Enable Google Cloud Print Proxy’ is set to ‘Disabled’

Rationale

Disabling this option will prevent users from printing documents from unmanaged devices to an organization’s printer.

Description

This setting enables Google Chrome to act as a proxy between Google Cloud Print and legacy printers connected to the machine.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Printing\Enable Google Cloud
Print Proxy
```

Impact:

If this setting is disabled, users cannot enable the proxy, and the machine will not be allowed to share its local printers with Google Cloud Print.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
  Google Cloud Print proxy
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: CloudPrintProxyEnabled
action: DWORD:0
```

R2.13

(L1) Ensure ‘Enable Site Isolation for every site’ is set to ‘Enabled’

(L1) Ensure ‘Enable Site Isolation for every site’ is set to ‘Enabled’

Rationale

Chrome will load each website in its own process. So, even if a site bypasses the same-origin policy, the extra security will help stop the site from stealing your data from another website.

Description

This policy controls is every website will load into its own process.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

`Computer Configuration\Administrative Templates\Google\Google Chrome\Enable Site Isolation for every site`

Impact:

If the policy is enabled, each site will run in its own process which will cause the system to use more memory. You might want to look at the IsolateOrigins policy setting to get the best of both worlds, isolation and limited impact for users, by using IsolateOrigins with a list of the sites you want to isolate.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
  Site Isolation for every site
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: SitePerProcess
action: DWORD:1
```

R2.14

(L1) Ensure ‘Allow download restrictions’ is set to ‘Enabled’ with ‘Block dangerous downloads’ specified.

(L1) Ensure ‘Allow download restrictions’ is set to ‘Enabled’ with ‘Block dangerous downloads’ specified.

Rationale

Users shall be prevented from downloading certain types of files, and shall not be able to bypass security warnings.

Description

Google Chrome allows to block certain types of downloads, and won’t let users bypass the security warnings, depending on the classification of Safe Browsing.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with value ‘Block dangerous downloads’ selected from drop down:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Allow download restrictions
```

Impact:

If this setting is enabled, all downloads are allowed, except for those that carry Safe Browsing warnings.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Allow
  download restrictions
value: Block dangerous downloads
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: DownloadRestrictions
action: DWORD:1
```

R2.15

(L1) Ensure ‘Disable proceeding from the Safe Browsing warning page’ is set to ‘Enabled’

(L1) Ensure ‘Disable proceeding from the Safe Browsing warning page’ is set to ‘Enabled’

Rationale

Malicious web pages are widely spread in the internet and pose the most significant threat to the user today. Users shall be prevented from navigating to potentially malicious web content.

Description

Google provides the Safe Browsing service. It shows a warning page when users navigate to sites that are flagged as potentially malicious.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Disable proceeding from the Safe Browsing warning page`

Impact:

Enabling this setting prevents users from proceeding anyway from the warning page to the malicious site. In some cases legitimate sites could be blocked and users would be prevented from accessing.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Disable
  proceeding from the Safe Browsing warning page
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: DisableSafeBrowsingProceedAnyway
action: DWORD:1
```

R2.16

(L1) Ensure ‘Notify a user that a browser relaunch or device restart is recommended or required’ is set to ‘Enabled’ with ‘Show a recurring prompt to the user indication that a relaunch is required’ specified

(L1) Ensure ‘Notify a user that a browser relaunch or device restart is recommended or required’ is set to ‘Enabled’ with ‘Show a recurring prompt to the user indication that a relaunch is required’ specified

Rationale

Security Updates shall be installed as soon as possible after release.

Description

Google Chrome offers to notify users that Google Chrome must be restarted to apply a pending update once the notification period defined by policy ‘Set the time period for update notifications’ is passed.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with value `Show a recurring prompt to the user indication that a relaunch is required` specified:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Notify a user that a browser relaunch or device restart is recommended or required`

Impact:

A recurring warning will be shown to the user indicating that a browser relaunch will be forced once the notification period passes. The user’s session is restored after the relaunch of Google Chrome.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Notify
  a user that a browser relaunch or device restart is recommended or required
value: Show a recurring prompt to the user indicating that a relaunch is required
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: RelaunchNotification
action: DWORD:2
```

R2.17

(L1) Ensure ‘Set the time period for update notifications’ is set to ‘Enabled’ with ‘86400000’ (1 day) specified

(L1) Ensure ‘Set the time period for update notifications’ is set to ‘Enabled’ with ‘86400000’ (1 day) specified

Rationale

Security Updates shall be installed as soon as possible after release.

Description

Google Chrome allows to set the time period, in milliseconds, over which users are notified that Google Chrome must be relaunched to apply a pending update.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with value `86400000` specified:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Set the time period for update notifications`

Impact:

Over this time period, the user will be repeatedly informed of the need for an update until a Browser restart is completed.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Set
  the time period for update notifications
value: 86400000
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: RelaunchNotificationPeriod
action: DWORD:86400000
```

R2.18

(L2) Ensure ‘Whether online OCSP/CRL checks are required for local trust anchors’ is set to ‘Enabled’

(L2) Ensure ‘Whether online OCSP/CRL checks are required for local trust anchors’ is set to ‘Enabled’

Rationale

Certificates shall always be validated.

Description

Google Chrome performs revocation checking for server certificates that successfully validate and are signed by locally-installed CA certificates. If Google Chrome is unable to obtain revocation status information, such certificates will be treated as revoked (‘hard-fail’).

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Whether online OCSP/CRL checks are required for local trust anchors`

Impact:

A revocation check will be performed for server certificates that successfully validate and are signed by locally-installed CA certificates. if the OCSP server goes down, then this will hard-fail and prevent browsing to those sites.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Whether
  online OCSP/CRL checks are required for local trust anchors
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: RequireOnlineRevocationChecksForLocalAnchors
action: DWORD:1
```

R2.19

(L1) Ensure ‘Enable Chrome Cleanup on Windows’ is Configured

(L1) Ensure ‘Enable Chrome Cleanup on Windows’ is Configured

Rationale

The Google Chrome Cleanup is ON by default and each organization should review and determine if they want to use this solutions for malware detection. If another solution is used instead of the built in Chrome option then an organization should configure the setting to Disabled.

Description

Chrome provides a Cleanup-feature to detect unwanted software. This feature periodically scans the system for unwanted software and will ask the user if they wish to remove it, if any been found.

01 Implementation Example

To establish the recommended configuration via Group Policy, configure the following setting to meet organizational requirements:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Enable Chrome Cleanup on Windows
```

Impact:

if Disabled, Chrome Cleanup will no longer be able to scan the system. If users do not have a centrally managed anti-malware solution then leaving this setting enabled can help protect a system.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
  Chrome Cleanup on Windows
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: ChromeCleanupEnabled
action: DWORD:1
```

R2.20

(L2) Ensure ‘Use built-in DNS client’ is set to ‘Disabled’

(L2) Ensure ‘Use built-in DNS client’ is set to ‘Disabled’

Rationale

The built-in DNS client shall not be used to circumvent the usage of a trusted DNS server.

Description

Google Chrome offers to use a built-in DNS client.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Use built-in DNS client
```

Impact:

Users will not be able to use Google DNS-over-TLS and (in future) DNS-over-HTTPS if you disable the Chrome DNS stack.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Use
  built-in DNS client
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: BuiltInDnsClientEnabled
action: DWORD:0
```

R2.21

(L1) Ensure ‘Update policy override’ is set to ‘Enabled’ with ‘Always allow updates (recommended)’ or ‘Automatic silent updates’ specified

(L1) Ensure ‘Update policy override’ is set to ‘Enabled’ with ‘Always allow updates (recommended)’ or ‘Automatic silent updates’ specified

Rationale

Software updates shall be applied as soon as they are available since they may include latest security patches.

Description

Google Update manages installation of available Google Chrome updates from Google. This setting allows to define whether updates are to be applied automatically. Depending on the business scenario updates shall be applied periodically or also if the user seeks for updates.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with value `Always allow updates (recommended)` or `Automatic silent updates only` selected from drop down:

`Computer Configuration\Administrative Templates\Google\Google Update\Applications\Google Chrome\Update policy override`

Impact:

Latest updates are automatically applied at least periodically.

01 Machine readable information

Compound automation

Carry out the following automations:

- **Windows GPO Setting**

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Update\Applications\Google
  Chrome Dev\Update policy override
value: Always allow updates
```

- **Windows GPO Setting**

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Update\Applications\Google
  Chrome Beta\Update policy override
value: Always allow updates
```

- **Windows GPO Setting**

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Update\Applications\Google\Google
  Chrome\Update policy override
value: Always allow updates
```

- **Windows GPO Setting**

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Update\Applications\Google
  Chrome Frame\Update policy override
value: Always allow updates
```

Compound automation

Carry out the following automations:

- **Windows Registry Setting**

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Google\Update
value_name: Update{401C381F-E0DE-4B85-8BD8-3F3F14FBDA57}
action: DWORD:1
```

- **Windows Registry Setting**

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Google\Update
value_name: Update{8237E44A-0054-442C-B6B6-EA0509993955}
action: DWORD:1
```

- **Windows Registry Setting**

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Google\Update
value_name: Update{8A69D345-D564-463C-AFF1-A69D9E530F96}
action: DWORD:1
```

- **Windows Registry Setting**

```
system: org.scapolite.implementation.windows_registry
config: Computer
registry_key: Software\Policies\Google\Update
value_name: Update{8BA986DA-5100-405E-AA35-86F34A02ACBF}
action: DWORD:1
```

Privacy

This section contains recommendations that help improve user privacy. Organizations should review these settings and any potential impacts to ensure they make sense within the environment since they restrict some browser functionality.

R3.1

(L2) Ensure ‘Default cookies setting’ is set to ‘Enabled’ (Keep cookies for the duration of the session)

(L2) Ensure ‘Default cookies setting’ is set to ‘Enabled’ (Keep cookies for the duration of the session)

Rationale

Permanently stored cookies may be used for malicious intent.

Description

Allows you to set whether websites are allowed to set local data. Setting local data can be either allowed for all websites or denied for all websites.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with `Keep cookies for the duration of the session` selected from the drop down.

`Computer Configuration\Administrative Templates\Google\Google Chrome\Content Settings\Default cookies setting`

Impact:

If this setting is enabled, cookies will be cleared when the session closes.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Content
  Settings\Default cookies setting
value: Keep cookies for the duration of the session
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: DefaultCookiesSetting
action: DWORD:4
```

R3.2

(L1) Ensure ‘Default geolocation setting’ is set to ‘Enabled’ with ‘Do not allow any site to track the users’ physical location’

(L1) Ensure ‘Default geolocation setting’ is set to ‘Enabled’ with ‘Do not allow any site to track the users’ physical location’

Rationale

From a privacy point of view it is not desirable to submit indicators regarding the location of the device, since the processing of this information cannot be determined. Furthermore, this may leak information about the network infrastructure around the device.

Description

Google Chrome supports to track the users’ physical location using GPS, data about nearby Wi-Fi access points or cellular signal sites/towers (even if you’re not using them), and your computer’s IP.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with `Do not allow any site to track the users' physical location` selected from the drop down:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Content Settings\Default geolocation setting`

Impact:

If this setting is disabled, chrome will no longer send data about nearby Wi-Fi access points or cellular signal sites/towers (even if you’re not using them), and your computer’s IP address to google.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Content
  Settings\Default geolocation setting
value: Do not allow any site to track the users' physical location
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: DefaultGeolocationSetting
action: DWORD:2
```

R3.3

(L1) Ensure ‘Enable Google Cast’ is set to ‘Disabled’

(L1) Ensure ‘Enable Google Cast’ is set to ‘Disabled’

Rationale

Google Cast may send the contents of tabs, sites or the desktop from the browser to non trusted devices on the local network segment.

Description

Google Cast allows to send the contents of tabs, sites or the desktop from the browser to a remote display and sound system.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Google Cast\Enable Google Cast`

Impact:

If this is disabled Google Cast is not activated and the toolbar icon is not shown.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Google
  Cast\Enable Google Cast
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: EnableMediaRouter
action: DWORD:0
```

R3.4

(L1) Ensure ‘Block third party cookies’ is set to ‘Enabled’

(L1) Ensure ‘Block third party cookies’ is set to ‘Enabled’

Rationale

Blocking third party cookies can help protect a user’s privacy by eliminating a number of website tracking cookies.

Description

Chrome allows cookies to be set by web page elements that are not from the domain in the user’s address bar. Enabling this feature prevents third party cookies from being set.

NOTE: Third Party Cookies and Tracking Protection are required for many business critical websites, including SalesForce and Office365.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Block third party cookies
```

Impact:

Enabling this setting prevents cookies from being set by web page elements that are not from the domain that is in the browser’s address bar.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Block
  third party cookies
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: BlockThirdPartyCookies
action: DWORD:1
```

R3.5

(L1) Ensure ‘Enable reporting of usage and crash-related data’ is set to ‘Disabled’

(L1) Ensure ‘Enable reporting of usage and crash-related data’ is set to ‘Disabled’

Rationale

Anonymous crash/usage data can be used to identify people, companies and information, which can be considered data exfiltration from company systems.

Description

This Setting controls anonymous reporting of usage and crash-related data about Google Chrome to Google.

NOTE: This policy is not available on Windows instances that are not joined to a Microsoft® Active Directory® domain.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

`Computer Configuration\Administrative Templates\Google\Google Chrome\Enable reporting of usage and crash-related data`

Impact:

If this setting is disabled, this information is not sent to Google.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
  reporting of usage and crash-related data
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: MetricsReportingEnabled
action: DWORD:0
```

R3.6

(L1) Ensure ‘Control how Chrome Cleanup reports data to Google’ is set to ‘Disabled’

(L1) Ensure ‘Control how Chrome Cleanup reports data to Google’ is set to ‘Disabled’

Rationale

Anonymous crash/usage data can be used to identify people, companies and information, which can be considered data exfiltration from company systems.

Description

Chrome provides a Cleanup-feature to detect unwanted software. The results of the cleanup may be shared with Google to assist with future unwanted software detection. These results will contain file metadata, automatically installed extensions and registry keys.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Control how Chrome Cleanup reports data to Google`

Impact:

Chrome Cleanup detected unwanted software, will no longer report metadata about the scan to Google.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Control
  how Chrome Cleanup reports data to Google
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: ChromeCleanupReportingEnabled
action: DWORD:0
```

R3.7

(L1) Ensure ‘Browser sign in settings’ is set to ‘Enabled’ with ‘Disabled browser sign-in’ specified

(L1) Ensure ‘Browser sign in settings’ is set to ‘Enabled’ with ‘Disabled browser sign-in’ specified

Rationale

Since external accounts are unmanaged and potentially used to access several private computer systems and many different websites, connecting accounts via sign-in poses a security risk for the company. It interferes with the corporate management mechanisms, as well as permits an unwanted leak of corporate information and possible mixture with private, non-company data.

Description

Google Chrome offers to sign-in with your Google account and use account related services like Chrome sync. It is possible to sign-in to Google Chrome with a Google account to use services like synchronization and can also be used for configuration and management of the browser.

NOTE: if an organization is a G Suite Enterprise customer they will want to leave this setting enabled so that users can sign in with Google accounts.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with value ‘Disabled browser sign-in’ selected from the drop down.

`Computer Configuration\Administrative Templates\Google\Google Chrome\Browser sign in settings`

Impact:

If this setting is enabled the user can not sign in to the browser and use google account based services like Chrome sync.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Browser
  sign in settings
value: Disable browser sign-in
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: BrowserSignin
action: DWORD:0
```

R3.8

(L1) Ensure ‘Enable Translate’ is set to ‘Disabled’

(L1) Ensure ‘Enable Translate’ is set to ‘Disabled’

Rationale

Content of internal web pages may be leaked to Google’s translation service.

Description

Content of internal web pages may be leaked to Google’s translation service.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Enable Translate`

Impact:

After disabling this feature Chrome contents of a web page are no longer sent to Google for translation.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
  Translate
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: TranslateEnabled
action: DWORD:0
```

R3.9

(L1) Ensure ‘Enable network prediction’ is set to ‘Enabled’ with ‘Do not predict actions on any network connection’ selected

(L1) Ensure ‘Enable network prediction’ is set to ‘Enabled’ with ‘Do not predict actions on any network connection’ selected

Rationale

Opening connections to resources which may never be visited shall be prevented.

Description

Google Chrome comes with the network prediction feature which provides DNS prefetching, TCP and SSL preconnection, and prerendering of web pages. This feature might lead to connections to websites which the user has not navigated to and may never visit.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` with value `Do not predict actions on any network connection` selected from the drop down:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Enable network prediction`

Impact:

Users will not be presented with web page predictions.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
  network prediction
value: Do not predict network actions on any network connection
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: NetworkPredictionOptions
action: DWORD:2
```

R3.10

(L1) Ensure ‘Enable search suggestions’ is set to ‘Disabled’

(L1) Ensure ‘Enable search suggestions’ is set to ‘Disabled’

Rationale

Using search suggestions may leak information as soon as it is typed/pasted into the omnibox, e.g. passwords, internal webservices, folder structures, etc.

Description

Google Chrome offers suggestions in Google Chrome’s omnibox while user is typing.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Enable search suggestions`

Impact:

The user has to send the search request actively by using the search button or hitting “Enter”.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
  search suggestions
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: SearchSuggestEnabled
action: DWORD:0
```

R3.11

(L1) Ensure ‘Enable or disable spell checking web service’ is set to ‘Disabled’

(L1) Ensure ‘Enable or disable spell checking web service’ is set to ‘Disabled’

Rationale

Information typed in may be leaked to Google’s spellcheck web service.

Description

Google Chrome offers the usage of a Google web service to help resolve spelling errors.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Enable or disable spell checking web service`

Impact:

After disabling this feature Chrome no longer sends the entire contents of text fields as you type in them to Google. Spell checking can still be performed using a downloaded dictionary; this policy only controls the usage of the online service.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
  or disable spell checking web service
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: SpellCheckServiceEnabled
action: DWORD:0
```

R3.12

(L1) Ensure ‘Enable alternate error pages’ is set to ‘Disabled’

(L1) Ensure ‘Enable alternate error pages’ is set to ‘Disabled’

Rationale

Using navigation suggestions may leak information about the web site intended to be visited.

Description

Google Chrome offers to show suggestions for the page you were trying to reach when it is unable to connect to a web address such as ‘Page Not Found’.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Enable alternate error pages`

Impact:

If this setting is disabled, Chrome does no longer use a web service to help resolve navigation errors.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
  alternate error pages
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: AlternateErrorPagesEnabled
action: DWORD:0
```

R3.13

(L1) Ensure ‘Disable synchronization of data with Google’ is set to ‘Enabled’

(L1) Ensure ‘Disable synchronization of data with Google’ is set to ‘Enabled’

Rationale

Browser data shall not be synchronized into the Google Cloud.

Description

Google Chrome offers to synchronize browser data using Google-hosted synchronization services.

NOTE: if your organization allows synchronization of data with Google, then enabling this setting will synchronize saved passwords with Google.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Disable synchronization of data with Google`

Impact:

If this setting is enabled, browser data will no longer sync with Google across devices/platforms allowing users to pick up where they left off.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Disable
  synchronization of data with Google
value: Enabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: SyncDisabled
action: DWORD:1
```

R3.14

(L1) Ensure ‘Enable Safe Browsing for trusted sources’ is set to ‘Disabled’

(L1) Ensure ‘Enable Safe Browsing for trusted sources’ is set to ‘Disabled’

Rationale

Information requested from trusted sources shall not be sent to Google’s safe browsing servers.

Description

Google Chrome can be adjusted to allow download without Safe Browsing checks when the requested files is from a trusted source. Trusted sources can be defined using policy ‘Configure the list of domains on which Safe Browsing will not trigger warnings’.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Enable Safe Browsing for trusted sources`

Impact:

If this setting is disabled files downloaded from intranet resources will not be checked by Google Services.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
  Safe Browsing for trusted sources
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: SafeBrowsingForTrustedSourcesEnabled
action: DWORD:0
```

R3.15

(L1) Ensure ‘Enable URL-keyed anonymized data collection’ is set to ‘Disabled’

(L1) Ensure ‘Enable URL-keyed anonymized data collection’ is set to ‘Disabled’

Rationale

Anonymized data collection shall be disabled, since it is unclear which information exactly is sent to Google.

Description

Google Chrome offers the feature URL-keyed anonymized data collection. This sends URLs of pages the user visits to Google to optimize its services.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Enable URL-keyed anonymized data collection`

Impact:

anonymized data will not be sent to Google to help optimize its services

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
  URL-keyed anonymized data collection
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: UrlKeyedAnonymizedDataCollectionEnabled
action: DWORD:0
```

R3.16

(L1) Ensure ‘Enable deleting browser and download history’ is set to ‘Disabled’

(L1) Ensure ‘Enable deleting browser and download history’ is set to ‘Disabled’

Rationale

If users can delete websites they have visited or files they have downloaded it will be easier for them to hide evidence that they have visited unauthorized or malicious sites.

Description

Google Chrome offer to delete the browser and download history using the clear browsing data menu.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Enable deleting browser and download history`

Impact:

If this setting is disabled, browsing and download history cannot be deleted by using the clear browsing data menu.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
  deleting browser and download history
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: AllowDeletingBrowserHistory
action: DWORD:0
```

Management/visibility/performance

This section contains recommendations around the management, visibility and performance of Google Chrome.

Remote access

This section contains recommendations that are related to remote access.

R4.1.1

(L1) Ensure ‘Enable firewall traversal from remote access host’ is set to ‘Disabled’

(L1) Ensure ‘Enable firewall traversal from remote access host’ is set to ‘Disabled’

Rationale

If this setting is enabled, remote clients can discover and connect to this machines even if they are separated by a firewall.

Description

Chrome enables the usage of STUN servers which allows remote clients to discover and connect to a machine even if they are separated by a firewall. By disabling this feature, in conjunction with filtering outgoing UDP connections, the machine will only allow connections from machines within the local network.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
Computer Configuration\Administrative Templates\Google\Google Chrome\Configure remote access
options\Enable firewall traversal from remote access host
```

Impact:

If this setting is disabled and outgoing UDP connections are filtered by the firewall, this machine will only allow connections from client machines within the local network.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Configure
  remote access options\Enable firewall traversal from remote access host
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: RemoteAccessHostFirewallTraversal
action: DWORD:0
```

R4.1.2

(L1) Ensure ‘Enable or disable PIN-less authentication for remote access hosts’ is set to ‘Disabled’

(L1) Ensure ‘Enable or disable PIN-less authentication for remote access hosts’ is set to ‘Disabled’

Rationale

If this setting is enabled or not configured, users can opt to pair clients and hosts at connection time, eliminating the need to enter a PIN every time.

Description

Chrome enables a user to opt-out of using user-specified PIN authentication and instead pair clients and hosts during connection time.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

`Computer Configuration\Administrative Templates\Google\Google Chrome\Configure remote access options\Enable or disable PIN-less authentication`

Impact:

If this setting is disabled, users will be required to enter PIN every time.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Configure
  remote access options\Enable or disable PIN-less authentication for remote access
  hosts
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: RemoteAccessHostAllowClientPairing
action: DWORD:0
```

R4.1.3

(L1) Ensure ‘Enable the use of relay servers by the remote access host’ is set to ‘Disabled’.

(L1) Ensure ‘Enable the use of relay servers by the remote access host’ is set to ‘Disabled’.

Rationale

Relay servers shall not be used to circumvent firewall restrictions.

Description

Google Chrome offers to use relay servers when clients are trying to connect to this machine and a direct connection is not available.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

`Computer Configuration\Administrative Templates\Google\Google Chrome\Configure remote access options\Enable the use of relay servers by the remote access host`

Impact:

If this setting is disabled, remote clients can not use relay servers to connect to this machine.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Configure
  remote access options\Enable the use of relay servers by the remote access host
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: RemoteAccessHostAllowRelayedConnection
action: DWORD:0
```

R4.1.4

(L1) Ensure ‘Configure the required domain names for remote access clients’ is set to ‘Enabled’ with a domain defined

(L1) Ensure ‘Configure the required domain names for remote access clients’ is set to ‘Enabled’ with a domain defined

Rationale

Remote assistance connections shall be restricted.

Description

Chrome allows the user to configure a list of required host domain that is imposed on remote access hosts. When enabled, hosts can only be shared using accounts that are registered to the specified domains.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled` and enter a domain (e.g. `nodomain.local`):

`Computer Configuration\Administrative Templates\Google\Google Chrome\Configure remote access options\Configure the required domain names for remote access clients`

Impact:

If this setting is enabled, clients from the specified domains only can connect to the host.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Configure
  remote access options\Configure the required domain names for remote access clients
value:
- nodomain.local
```

Compound automation

Carry out the following automations:

- **Windows Registry Setting**

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome\RemoteAccessHostClientDomainList
value_name: '*'
action: DELETEALLVALUES
```

- **Windows Registry Setting**

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome\RemoteAccessHostClientDomainList
value_name: '1'
action: SZ:nodomain.local
```

Data Loss Prevention

This section contains recommendations to help prevent and protect against unwanted loss of data. Organizations should review these settings and any potential impacts to ensure they makes sense within the environment since they so restrict some browser functionality.

R5.1

(L1) Ensure ‘Enable submission of documents to Google Cloud print’ is set to ‘Disabled’

(L1) Ensure ‘Enable submission of documents to Google Cloud print’ is set to ‘Disabled’

Rationale

Disabling this option will prevent users from printing possible confidential enterprise documents through the cloud.

Description

This setting enables Google Chrome to submit documents to Google Cloud Print for printing.

NOTE: This only affects Google Cloud Print support in Google Chrome. It does not prevent users from submitting print jobs on web sites.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

`Computer Configuration\Administrative Templates\Google\Google Chrome\Printing\Enable submission of documents to Google Cloud print`

Impact:

If this setting is disabled, users cannot print to Google Cloud Print from the Chrome print dialog

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
  submission of documents to Google Cloud Print
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: CloudPrintSubmitEnabled
action: DWORD:0
```

R5.2

(L1) Ensure ‘Import saved passwords from default browser on first run’ is set to ‘Disabled’

(L1) Ensure ‘Import saved passwords from default browser on first run’ is set to ‘Disabled’

Rationale

In Chrome, passwords can be stored in plain-text and revealed by clicking the “show” button next to the password field by going to chrome://settings/passwords/.

Description

This setting controls if saved passwords from the default browser can be imported.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

`Computer Configuration\Administrative Templates\Google\Google Chrome\Import saved passwords from default browser on first run`

Impact:

If this setting is disabled, saved passwords from other browsers are not imported.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Import
  saved passwords from default browser on first run
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: ImportSavedPasswords
action: DWORD:0
```

R5.3

(L1) Ensure ‘Enable AutoFill for credit cards’ is set to ‘Disabled’

(L1) Ensure ‘Enable AutoFill for credit cards’ is set to ‘Disabled’

Rationale

If an attacker gains access to a user’s machine where the user has stored credit card AutoFill data, information could be harvested.

Description

Chrome allows users to auto-complete web forms with saved credit card information. Disabling this feature will prompt a user to enter all information manually.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`:

`Computer Configuration\Administrative Templates\Google\Google Chrome\Enable AutoFill for credit cards`

Impact:

If this setting is disabled, credit card AutoFill will be inaccessible to users.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
  AutoFill for credit cards
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: AutofillCreditCardEnabled
action: DWORD:0
```

R5.4

(L1) Ensure ‘Enable AutoFill for addresses’ is set to ‘Disabled’

(L1) Ensure ‘Enable AutoFill for addresses’ is set to ‘Disabled’

Rationale

If an attacker gains access to a user’s machine where the user has stored address AutoFill data, information could be harvested.

Description

Chrome allows users to auto-complete web forms with saved information such as address or phone number. Disabling this feature will prompt a user to enter all information manually.

01 Implementation Example

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

`Computer Configuration\Administrative Templates\Google\Google Chrome\Enable AutoFill for addresses`

Impact:

If this setting is disabled, AutoFill will be inaccessible to users.

01 Machine readable information

Windows GPO Setting

```
ui_path: Computer Configuration\Administrative Templates\Google\Google Chrome\Enable
  AutoFill for addresses
value: Disabled
```

Windows Registry Setting

```
system: org.scapolite.implementation.windows_registry
config: Both
registry_key: Software\Policies\Google\Chrome
value_name: AutofillAddressEnabled
action: DWORD:0
```

References