



CVE-2016-5134

Published on: 07/23/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:09 PM UTC

CVE-2016-5134

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Chrome](#) from [Google](#) contain the following vulnerability:

net/proxy/proxy_service.cc in the Proxy Auto-Config (PAC) feature in Google Chrome before 52.0.2743.82 does not ensure that URL information is restricted to a scheme, host, and port, which allows remote attackers to discover credentials by operating a server with a PAC script, a related issue to CVE-2016-3763.

CVE-2016-5134 has been assigned by [Google](#) security@google.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Chromium: Multiple vulnerabilities (GLSA 201610-09) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201610-09
Google Chrome Multiple Flaws Lets Remote	www.securitytracker.com	SECTrack 1036428

Google Chrome Multiple flaws L&ES Remote Users Bypass Same-Origin Restrictions, Obtain Potentially Sensitive Information, Spoof URLs, and Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECURITYTRACKER 1000420
[security-announce] openSUSE-SU-2016:1865-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1865
USN-3041-1: Oxide vulnerabilities Ubuntu	www.ubuntu.com text/html	UBUNTU USN-3041-1
Issue 1996773002: Sanitize https:// URLs before sending them to PAC scripts. - Code Review	Issue Tracking codereview.chromium.org text/html	CONFIRM codereview.chromium.org/1996773002
Debian -- Security Information -- DSA-3637-1 chromium-browser	www.debian.org Deprecated Link text/html	DEBIAN DSA-3637
Google Chrome Prior to 52.0.2743.82 Multiple Security Vulnerabilities	cve.report (archive) text/html	BID 92053
[security-announce] openSUSE-SU-2016:1869-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1869
Vulnerability Note VU#877625 - Proxy auto-config (PAC) files have access to full HTTPS URLs	www.kb.cert.org text/html	CERT-VN VU#877625
Chrome Releases: Stable Channel Update	Vendor Advisory googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2016/07/stable-channel-update.html
[security-announce] openSUSE-SU-2016:1918-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1918
593759 - Security: Proxy Auto-Config SSL/TLS Url Disclosure - chromium - Monorail	crbug.com text/html	CONFIRM crbug.com/593759
[security-announce] openSUSE-SU-2016:1868-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:1868
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1485

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Chrome	All	All	All	All
cpe:2.3:a:google:chrome:*****:*						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)