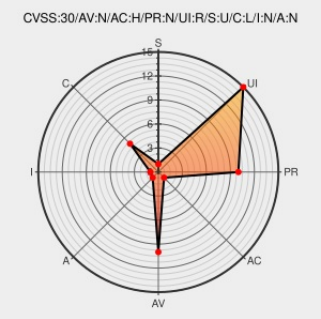
CVE-2016-5166

Published on: 09/11/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:10 PM UTC

CVE-2016-5166

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Chrome from Google contain the following vulnerability:

The download implementation in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not properly restrict saving a file:// URL that is referenced by an http:// URL, which makes it easier for user-assisted remote attackers to discover NetNTLM hashes and conduct SMB relay attacks via a crafted web page that is accessed with the "Save page as" menu choice.

CVE-2016-5166 has been assigned by security@google.com to track the vulnerability - currently rated as LOW severity.

CVSS3 Score: 3.1 - LOW

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

CVSS2 Score: 2.6 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Issue 2075273002: Resource requests from Save-Page-As should go through	Issue Tracking codereview.chromium.org	CONFIRM codereview.chromium.org/2075273002

CanRequestURL checks. - Code Review	text/html	
Chromium: Multiple vulnerabilities (GLSA 201610-09) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201610-09
[security-announce] openSUSE-SU-2016:2250-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:2250
[security-announce] openSUSE-SU-2016:2296-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:2296
openSUSE-SU-2016:2349-1: moderate: Security update for opera	Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2016:2349
Chrome Releases: Stable Channel Update for Desktop	Vendor Advisory googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2016/08/stable-channel-update-for-desktop_31.html
[security-announce] SUSE-SU-2016:2251-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:2251
Debian -- Security Information -- DSA-3660-1 chromium-browser	www.debian.org Depreciated Link text/html	DEBIAN DSA-3660
Google Chrome Multiple Flaws Lets Remote Users Bypass Security Restrictions, Conduct Cross-Site Scripting Attacks, Spoof URLs, and Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1036729
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:1854
Google Chrome Prior to 53.0.2785.89 Multiple Security Vulnerabilities	cve.report (archive) text/html	BID 92717
616429 - Security: Saving WebPage with file: resources access SMB resources - chromium - Monorail	Permissions Required crbug.com text/html	CONFIRM crbug.com/616429

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
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All

cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→