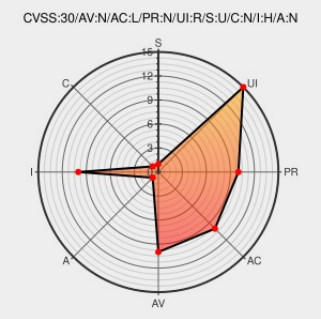
CVE-2018-17460

Published on: 06/27/2019 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:54:00 AM UTC

CVE-2018-17460

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



Certain versions of Chrome from Google contain the following vulnerability:

Insufficient data validation in filesystem URIs in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.

CVE-2018-17460 has been assigned by security@google.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Google** - **Chrome** version **< 68.0.3440.75**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Chrome Releases: Stable Channel Update for Desktop	chromereleases.googleblog.com text/html	MISC chromereleases.googleblog.com/2018/07/stable-channel-update-for-desktop.html

696446 - chromium - An open-source project to help move the web forward. - Monorail	Exploit Issue Tracking Vendor Advisory crbug.com text/html	MISC crbug.com/696446

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
Application	Google	Chrome	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→