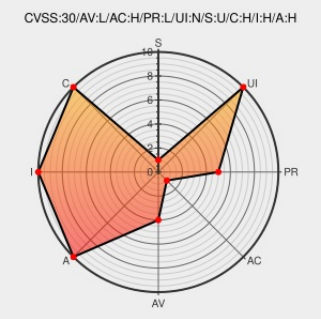
CVE-2017-15405

Published on: 01/09/2019 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:39:00 AM UTC

CVE-2017-15405

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



Certain versions of Chrome from Google contain the following vulnerability:

Inappropriate symlink handling and a race condition in the stateful recovery feature implementation could lead to a persistance established by a malicious code running with root privileges in cryptohomed in Google Chrome on Chrome OS prior to 61.0.3163.113 allowed a local attacker to execute arbitrary code via a crafted HTML page.

CVE-2017-15405 has been assigned by security@google.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Google** - **Chrome** version **< 61.0.3163.113**

CVSS3 Score: 7 - HIGH

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

CVSS2 Score: 6.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link

766276 - chromium - An open-source project to help move the web forward. - Monorail	crbug.com text/html	MISC crbug.com/766276
Chrome Releases: Stable Channel Updates for Chrome OS	chromereleases.googleblog.com text/html	CONFIRM chromereleases.googleblog.com/2017/10/stable-channel-updates-for-chrome-os.html

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→