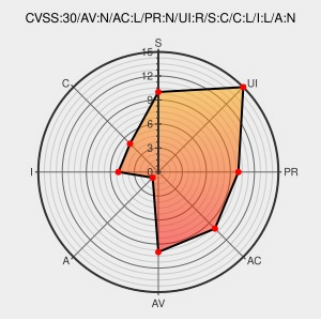
CVE-2018-20071

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

Last Modified on: 11/07/2023 02:56:00 AM UTC

CVE-2018-20071

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



Certain versions of Chrome from Google contain the following vulnerability:

Insufficiently strict origin checks during JIT payment app installation in Payments in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to install a service worker for a domain that can host attacker controled files via a crafted HTML page.

CVE-2018-20071 has been assigned by security@google.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Google** - **Chrome** version **< 70.0.3538.67**

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	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
853937 - chromium - An open-source project to help move the web forward. - Monorail	crbug.com text/html	MISC crbug.com/853937

Chrome Releases: Stable Channel Update for Desktop	chromereleases.googleblog.com text/html	CONFIRM chromereleases.googleblog.com/2018/12/stable-channel-update-for-desktop.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→