

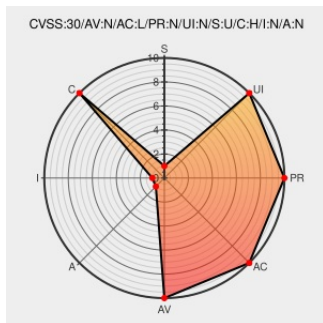


CVE-2017-18354

Published on: 12/17/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:55 PM UTC

CVE-2017-18354

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

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

Rendertron 1.0.0 allows for alternative protocols such as 'file:/' introducing a Local File Inclusion (LFI) bug where arbitrary files can be read by a remote attacker.

CVE-2017-18354 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
fix: clean errors, add validation & reduce exposed by a335926a · Pull Request #88 · GoogleChrome/rendertron · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/GoogleChrome/rendertron/pull/88

copyright headers (#72) ·
GoogleChrome/rendertron@8d70628
· GitHub

Patch
github.com
text/html

MISC
github.com/GoogleChrome/rendertron/commit/8d70628c96ae72eff6eebb451d26

759111 - chromium - An open-source project to help move the web forward. - Monorail

Exploit
Issue Tracking
Vendor Advisory
bugs.chromium.org
text/html

MISC bugs.chromium.org/p/chromium/issues/detail?id=759111

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.

Related QID Numbers

981019 Nodejs (npm) Security Update for rendertron (GHSA-j87c-cj65-vmh5)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Rendertron	1.0.0	All	All	All
Application	Google	Rendertron	1.0.0	All	All	All
cpe:2.3:a:google:rendertron:1.0.0:*:*:*:*:*:						
cpe:2.3:a:google:rendertron:1.0.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→