



CVE-2018-12911

Published on: 07/19/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:24 PM UTC

CVE-2018-12911

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

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

WebKitGTK+ 2.20.3 has an off-by-one error, with a resultant out-of-bounds write, in the `get_simple_globs` functions in `ThirdParty/xdgmime/src/xdgmimecache.c` and `ThirdParty/xdgmime/src/xdgmimeglob.c`.

CVE-2018-12911 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Changeset 233404 – WebKit	Patch Vendor Advisory trac.webkit.org text/html	MISC trac.webkit.org/changeset/233404/webkit

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Application	WebKitgtk	WebKitgtk	2.20.3	All	All	All
Application	WebKitgtk	WebKitgtk	2.20.3	All	All	All
Application	WebKitgtk	WebKitgtk	2.20.3	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:its:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:its:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:its:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:its:*:*:						
cpe:2.3:a:webkitgtk:webkitgtk+:2.20.3:*:*:*:*:*:						
cpe:2.3:a:webkitgtk:webkitgtk\+:2.20.3:*:*:*:*:*:						
cpe:2.3:a:webkitgtk:webkitgtk\+:2.20.3:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)