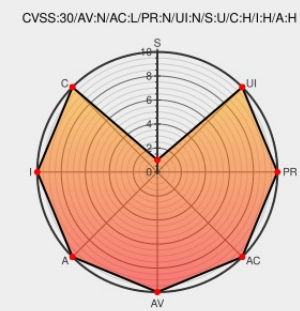
CVE-2017-1000121

Published on: 11/01/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:36 PM UTC

CVE-2017-1000121

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



Certain versions of Webkitgtk from Webkitgtk contain the following vulnerability:

The UNIX IPC layer in WebKit, including WebKitGTK+ prior to 2.16.3, does not properly validate message size metadata, allowing a compromised secondary process to trigger an integer overflow and subsequent buffer overflow in the UI process. This vulnerability does not affect Apple products.

CVE-2017-1000121 has been assigned by 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
WebKitGTK+ Security Advisory WSA-2017-0007 - The WebKitGTK+ Project	Vendor Advisory, webkitgtk.org, text/html	MISC webkitgtk.org/security/WSA-2017-0007.html

Changeset 217126 – WebKit

Third Party Advisory
trac.webkit.org
text/html

CONFIRM
trac.webkit.org/changeset/217126/webkit

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Webkitgtk	Webkitgtk	All	All	All	All
Application	Webkitgtk	Webkitgtk	All	All	All	All
Application	Webkitgtk	Webkitgtk	All	All	All	All

cpe:2.3:a:webkitgtk:webkitgtk+:*:*:*:*:*:*:*:*:

cpe:2.3:a:webkitgtk:webkitgtk\+:*:*:*:*:*:*:*:*:

cpe:2.3:a:webkitgtk:webkitgtk\+:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→