

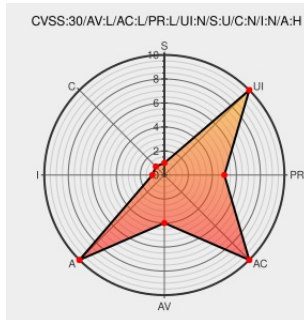


CVE-2017-11171

Published on: 07/11/2017 12:00:00 AM UTC

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

CVE-2017-11171

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

Certain versions of [Gnome-session](#) from [Gnome](#) contain the following vulnerability:

Bad reference counting in the context of `accept_ice_connection()` in `gsm-xsmp-server.c` in old versions of `gnome-session` up until version 2.29.92 allows a local attacker to establish ICE connections to `gnome-session` with invalid authentication data (an invalid magic cookie). Each failed authentication attempt will leak a file descriptor in `gnome-session`.

When the maximum number of file descriptors is exhausted in the `gnome-session` process, it will enter an infinite loop trying to communicate without success, consuming 100% of the CPU. The graphical session associated with the `gnome-session` process will stop working correctly, because communication with `gnome-session` is no longer possible.

CVE-2017-11171 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

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

CVSS2 Score: **4.9 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description

[gsm] Delay the creation of the GsmXSMPClient until it really exists · GNOME/gnome-session@b0dc999 · GitHub

Tags

Third Party Advisory

github.com

text/html

Link

 CONFIRM github.com/GNOME/gnome-session/commit/b0dc999e0b45355314616321dbb6cb71e729fc9d

Description

Bug 1025068 – VUL-0: CVE-2017-2626: libICE: Weak Entropy Usage in Session Keys in libICE

Tags

Issue Tracking

Third Party Advisory

bugzilla.suse.com

text/html

Link

 CONFIRM bugzilla.suse.com/show_bug.cgi?id=1025068

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
Application	Gnome	Gnome-session	All	All	All	All

cpe:2.3:a:gnome:gnome-session:*.***.***.***:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →