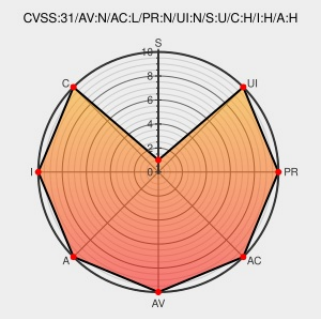
CVE-2019-15522

Published on: 03/20/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:45 PM UTC

CVE-2019-15522

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



Certain versions of Csync2 from Linbit contain the following vulnerability:

An issue was discovered in LINBIT csync2 through 2.0. csync_daemon_session in daemon.c neglects to force a failure of a hello command when the configuration requires use of SSL.

CVE-2019-15522 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
fail HELLO command when SSL is required · LINBIT/csync2@416f1de · GitHub	Patch, Vendor Advisory, github.com, text/html	MISC github.com/LINBIT/csync2/commit/416f1de878ef97e27e27508914f7ba8599a0be22

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

501833 Alpine Linux Security Update for csync2

750169 OpenSUSE Security Update for csync2 (openSUSE-SU-2021:0853-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linbit	Csync2	All	All	All	All

cpe:2.3:a:linbit:csync2:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→