



CVE-2019-15523

Published on: 12/30/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:44 PM UTC

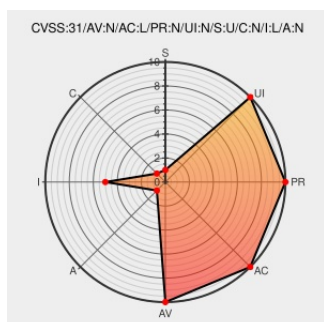
CVE-2019-15523

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

An issue was discovered in LINBIT csync2 through 2.0. It does not correctly check for the return value GNUTLS_E_WARNING_ALERT_RECEIVED of the gnutls_handshake() function. It neglects to call this function again, as required by the design of the API.

CVE-2019-15523 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
[SECURITY] [DLA 2515-1] csync2 security update	Mailing List Third Party Advisory lists.debian.org	MLIST [debian-lts-announce] 20210104 [SECURITY] [DLA 2515-1] csync2 security update

text/html

some security
improvements by
maltek · Pull Request
#13 · LINBIT/csync2 ·
GitHub

Patch

Third Party Advisory

github.com

text/html



MISC

github.com/LINBIT/csync2/pull/13/commits/92742544a56bcbcd9ec99ca15f898b31797e39e2

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
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Linbit	Csync2	All	All	All	All
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:a:linbit:csync2:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#)