



CVE-2020-29394

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-29394
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-30 19:15:00 UTC
Updated	2023-02-03 18:42:00 UTC
Description	A buffer overflow in the dlt_filter_load function in dlt_common.c from dlt-daemon through 2.18.5 (GENIVI Diagnostic Log an

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Dlt-daemon Project	Dlt-daemon	2.18.5	All	All	All
Application	Dlt-daemon Project	Dlt-daemon	All	All	All	All
Application	Genivi	Diagnostic Log And Trace	All	All	All	All

References

Reference	Source
fscanf() uses dynamic formatting to prevent buffer overflow by Kevin-Luong · Pull Request #288 · GENIVI/dlt-daemon · GitHub	MISC
[SECURITY] [DLA 3231-1] dlt-daemon security update	MLIST
dlt_common: Fix buffer overflow in dlt_filter_load by gy741 · Pull Request #275 · GENIVI/dlt-daemon · GitHub	MISC
stack buffer overflow in dlt_filter_load · Issue #274 · GENIVI/dlt-daemon · GitHub	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[180774](#) Debian Security Update for dlt-daemon (CVE-2020-29394)

[181308](#) Debian Security Update for dlt-daemon (DLA 3231-1)

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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