



CVE-2020-36244

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

Summary

CVE	CVE-2020-36244
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-10 07:15:00 UTC
Updated	2023-02-03 19:12:00 UTC
Description	The daemon in GENIVI diagnostic log and trace (DLT), is vulnerable to a heap-based buffer overflow that could allow an att

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	Genivi	Diagnostic Log And Trace	All	All	All	All
Application	Genivi	Diagnostic Log And Trace	All	All	All	All

References

Reference	Source	Link	Tags
write heap buffer overflow in dlt_buffer_write_block · Issue #265 · GENIVI/dlt-daemon · GitHub	MISC	github.com	Third Party A
[SECURITY] [DLA 3231-1] dlt-daemon security update	MLIST	lists.debian.org	
Comparing v2.18.5...v2.18.6 · GENIVI/dlt-daemon · GitHub	MISC	github.com	Patch, Third
GENIVI Alliance DLT CISA	MISC	us-cert.cisa.gov	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[180783](#) Debian Security Update for dlt-daemon (CVE-2020-36244)

© [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](#)