



CVE-2019-7146

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

Summary

CVE	CVE-2019-7146
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-01-29 00:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	In elfutils 0.175, there is a buffer over-read in the ebl_object_note function in eblobjnote.c in libebl. Remote attackers could

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Elfutils Project	Elfutils	0.175	All	All	All
Application	Elfutils Project	Elfutils	0.175	All	All	All

References

Reference	Source	Link	Tags
24081 – buffer over-read Problem in elf32_xlatetom function in libelf	MISC	sourceware.org	Exploit
Red Hat Customer Portal	REDHAT	access.redhat.com	
24075 – Program Crash due to buffer over-read in ebl_object_note function in eblobjnote.c in libebl.	MISC	sourceware.org	Exploit
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[377416](#) Alibaba Cloud Linux Security Update for elfutils (ALINUX3-SA-2022:0041)

[500175](#) Alpine Linux Security Update for elfutils

[500140](#) Alpine Linux Security Update for elfutils

© [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](#)