



CVE-2023-31284

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

Summary

CVE	CVE-2023-31284
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-04 20:15:00 UTC
Updated	2023-09-14 18:15:00 UTC
Description	illumos illumos-gate before 676abcb has a stack buffer overflow in /dev/net, leading to privilege escalation via a stat on a lo

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	illumos	illumos-gate	All	All	All	All

References

Reference	Source	Link	Tags
oss-security - Re: illumos (or at least danmcd) membership in the distros list	MLIST	www.openwall.com	
oss-security - Re: illumos (or at least danmcd) membership in the distros list	MLIST	www.openwall.com	
GitHub - illumos/illumos-gate at 16b76d3cb933ff92018a2a75594449010192each	MISC	github.com	
Topicbox	MISC	illumos.topicbox.com	
oss-security - illumos (or at least danmcd) membership in the distros list	MLIST	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

296099 Oracle Solaris 11.4 Support Repository Update (SRU) 57.144.3 Missing (CPUAPR2023)

© [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](#).

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