CVE-2022-2469

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-2469
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-19 16:15:00 UTC
Updated	2022-10-26 02:54:00 UTC
Description	GNU SASL libgsasl server-side read-out-of-bounds with malicious authenticated GSS-API client

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Gnu	Gnu Sasl	All	All	All	All
Application	Gnul	Gnu Sasl	All	All	All	All

References

Reference	Source	Link
GSSAPI server: Boundary check gss_wrap token (read OOB). (796e4197) · Commits · gsasl / gsasl · GitLab	MISC	gitlab.com
2022/CVE-2022-2469.json · master · GitLab.org / cves · GitLab	CONFIRM	gitlab.com
Debian -- Security Information -- DSA-5189-1 gsasl	DEBIAN	www.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Simon Josefsson

Legacy QID Mappings

180898 Debian Security Update for gsasl (DSA 5189-1)

184925 Debian Security Update for gsasl (CVE-2022-2469)

199486 Ubuntu Security Notification for GNU SASL Vulnerability (USN-6169-1)

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report