



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 gssasl (DSA 5189-1)

[184925](#) Debian Security Update for gssasl (CVE-2022-2469)

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

© [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](#)