



CVE-2023-25563

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

Summary

CVE	CVE-2023-25563
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-14 18:15:00 UTC
Updated	2023-02-22 18:37:00 UTC
Description	GSS-NTLMSSP is a mechglue plugin for the GSSAPI library that implements NTLM authentication. Prior to version 1.2.0, n

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gss-ntlmssp Project	Gss-ntlmssp	All	All	All	All

References

Reference	Source	Link	Tags
Multiple out-of-bounds read when decoding NTLM fields · Advisory · gssapi/gss-ntlmssp · GitHub	MISC	github.com	
Release Patched several CVEs reported by GitHub Security Lab · gssapi/gss-ntlmssp · GitHub	MISC	github.com	
Out-of-bounds read in multiple decode functions · gssapi/gss-ntlmssp@97c62c6 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160669](#) Oracle Enterprise Linux Security Update for gssntlmssp (ELSA-2023-3097)

[182576](#) Debian Security Update for gss-ntlmssp (CVE-2023-25563)

[241488](#) Red Hat Update for gssntlmssp (RHSA-2023:3097)

283735 Fedora Security Update for gssntlmssp (FEDORA-2023-cb63c0f615)
378651 Alibaba Cloud Linux Security Update for gssntlmssp (ALINUX3-SA-2023:0068)
941109 AlmaLinux Security Update for gssntlmssp (ALSA-2023:3097)

© [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](#)