



CVE-2023-25566

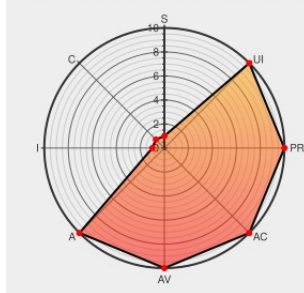
Published on: Not Yet Published

Last Modified on: 02/22/2023 06:39:00 PM UTC

CVE-2023-25566 - advisory for GHSA-mfm4-6g58-jw74

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H



Certain versions of [Gss-ntlmssp](#) from [Gss-ntlmssp Project](#) contain the following vulnerability:

GSS-NTLMSSP is a mechglue plugin for the GSSAPI library that implements NTLM authentication. Prior to version 1.2.0, a memory leak can be triggered when parsing usernames which can trigger a denial-of-service. The domain portion of a username may be overridden causing an allocated memory area the size of the domain name to be

leaked. An attacker can leak memory via the main `gss\_accept\_sec\_context` entry point, potentially causing a denial-of-service. This issue is fixed in version 1.2.0.

CVE-2023-25566 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [gssapi](#) - [gss-ntlmssp](#) version = < 1.2.0

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVE References

Description	Tags	Link
Release Patched several CVEs reported by GitHub Security Lab · gssapi/gss-ntlmssp · GitHub	github.com text/html	MISC github.com/gssapi/gss-ntlmssp/releases/tag/v1.2.0
GHSL-2023-010: Memory leak when parsing usernames · gssapi/gss-ntlmssp@8660fb1 · GitHub	github.com text/html	MISC github.com/gssapi/gss-ntlmssp/commit/8660fb16474054e692a596e9c79670cd4d3954f4
Memory leak when parsing usernames · Advisory · gssapi/gss-ntlmssp · GitHub	github.com text/html	MISC github.com/gssapi/gss-ntlmssp/security/advisories/GHSA-mfm4-6g58-jw74

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that

would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

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

184237 Debian Security Update for gss-ntlmssp (CVE-2023-25566)

[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 qssntlmssp (ALSA-2023:3097)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gss-ntlmssp Project	Gss-ntlmssp	All	All	All	All
cpe:2.3:a:gss-ntlmssp_project:gss-ntlmssp:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 /r/netcve	CVE-2023-25566	2023-02-14 19:38:15

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

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