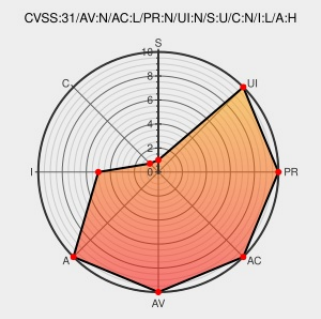
CVE-2023-25564

Published on: Not Yet Published

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

CVE-2023-25564 - advisory for GHSA-r85x-q5px-9xfq

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



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, memory corruption can be triggered when decoding UTF16 strings. The variable `outlen` was not initialized and could cause writing a zero to an arbitrary place in memory if `ntlm_str_convert()` were to fail, which would leave `outlen` uninitialized. This can lead to a denial of service if the write hits unmapped memory or randomly corrupts a byte in the application memory space. This vulnerability can trigger an out-of-bounds write, leading to memory corruption. This vulnerability can be triggered via the main `gss_accept_sec_context` entry point. This issue is fixed in version 1.2.0.

CVE-2023-25564 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: 8.2 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	LOW	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-2023-013: Memory corruption decoding UTF16 · gssapi/gss-ntlmssp@c753000 · GitHub	github.com text/html	MISC github.com/gssapi/gss-ntlmssp/commit/c753000eb31835c0664e528fbc99378ae0cbe950

Memory corruption when decoding UTF16 strings · Advisory · gssapi/gss-ntlmssp · GitHub	github.com text/html	MISC github.com/gssapi/gss-ntlmssp/security/advisories/GHSA-r85x-q5px-9xfq

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)

183524 Debian Security Update for gss-ntlmssp (CVE-2023-25564)

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)

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-2023-25564	2023-02-14 18:38:35

← Previous ID

Next ID→

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