



# Potential buffer overflow in ns\_sprintf TSIG handling path

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

## Summary

<b>CVE</b>	CVE-2026-5435
<b>State</b>	PUBLISHED
<b>Assigner</b>	glibc
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-28 13:19:22 UTC
<b>Updated</b>	2026-05-05 17:38:37 UTC
<b>Description</b>	The deprecated functions ns_printf, ns_print and fp_nquery in the GNU C Library version 2.2 and newer fail to enforce tr

## Risk And Classification

**Primary CVSS:** v3.1 7.3 HIGH from ADP

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

**EPSS:** 0.000490000 probability, percentile 0.148400000 (date 2026-05-05)

**Problem Types:** CWE-787 | CWE-787 CWE-787 Out-of-bounds write

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Glibc	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	The GNU C Library	Glibc	affected 2.2 * custom	Not specified

### References

Reference	Source	Li
<a href="https://inbox.sourceware.org/libc-announce/7a655d55-276f-41fe-b550-feb3ebb2ce91@redhat.com/T">inbox.sourceware.org/libc-announce/7a655d55-276f-41fe-b550-feb3ebb2ce91@redhat.com/T</a>	3ff69d7a-14f2-4f67-a097-88dee7810d18	inl
<a href="https://sourceware.org/bugzilla/show_bug.cgi">sourceware.org/bugzilla/show_bug.cgi</a>	3ff69d7a-14f2-4f67-a097-88dee7810d18	sc
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nv

### Vendor Comments And Credit

Discovery Credit

**CNA:** shinobu (en)

There are currently no legacy QID mappings associated with this CVE.

© 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](#)