



# scanf %mc off-by-one heap buffer overflow

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

## Summary

<b>CVE</b>	CVE-2026-5450
<b>State</b>	PUBLISHED
<b>Assigner</b>	glibc
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-20 21:16:36 UTC
<b>Updated</b>	2026-04-20 21:16:36 UTC
<b>Description</b>	Calling the scanf family of functions with a %mc (malloc'd character match) in the GNU C Library version 2.7 to version 2.4...

## Risk And Classification

**Problem Types:** CWE-122 | CWE-122 CWE-122 Heap-based buffer overflow

## Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">The GNU C Library</a>	Glibc	affected 2.7 * custom	Not specified

## References

Reference	Source	
<a href="https://inbox.sourceware.org/libc-announce/b11f0003-6ec1-4bd6-b9de-9e38a4efeca3@redhat.com/T">inbox.sourceware.org/libc-announce/b11f0003-6ec1-4bd6-b9de-9e38a4efeca3@redhat.com/T</a>	3ff69d7a-14f2-4f67-a097-88dee7810d18	in
<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	n

## Vendor Comments And Credit

Discovery Credit

**CNA:** Rocket Ma (en)

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)