scanf %mc off-by-one heap buffer overflow

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-5450
State	PUBLISHED
Assigner	glibc
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-20 21:16:36 UTC
Updated	2026-04-20 21:16:36 UTC
Description	Calling the scanf family of functions with a %mc (malloc'd character match) in the GNU C Library version 2.7 to version 2.43

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	The GNU C Library	Glibc	affected 2.7 * custom	Not specified

References

Reference	Source	L
inbox.sourceware.org/libc-announce/b11f0003-6ec1-4bd6-b9de-9e38a4efeca3@redhat.com/T	3ff69d7a-14f2-4f67-a097-88dee7810d18	in
sourceware.org/bugzilla/show_bug.cgi	3ff69d7a-14f2-4f67-a097-88dee7810d18	s
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.

Free CVE JSON API cve.report/api

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