CVE-2023-36660

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-36660
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-25 22:15:00 UTC
Updated	2023-07-03 19:20:00 UTC
Description	The OCB feature in libnettle in Nettle 3.9 before 3.9.1 allows memory corruption.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nettle Project	Nettle	3.9	All	All	All

References

Reference	Source	Link	Tags
nettle_3.9_release_20230514...nettle_3.9.1_release_20230601 · Nettle / nettle · GitLab	MISC	git.lysator.liu.se	
1212112 – VUL-0: libnettle: the new OCB code may be exploitable due to memory corruption	MISC	bugzilla.suse.com	
Fix ocb loop for processing larger messages. (867a4548) · Commits · Nettle / nettle · GitLab	MISC	git.lysator.liu.se	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710842 Gentoo Linux Nettle Denial of Service (DoS) Vulnerability (GLSA 202401-24)

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