



# CVE-2023-36660

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

## Summary

<b>CVE</b>	CVE-2023-36660
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-06-25 22:15:00 UTC
<b>Updated</b>	2023-07-03 19:20:00 UTC
<b>Description</b>	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	<a href="#">Nettle Project</a>	<a href="#">Nettle</a>	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	<a href="https://git.lysator.liu.se">git.lysator.liu.se</a>	
1212112 – VUL-0: libnettle: the new OCB code may be exploitable due to memory corruption	MISC	<a href="https://bugzilla.suse.com">bugzilla.suse.com</a>	
Fix ocb loop for processing larger messages. (867a4548) · Commits · Nettle / nettle · GitLab	MISC	<a href="https://git.lysator.liu.se">git.lysator.liu.se</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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)

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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**