



# CVE-2021-41040

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

## Summary

<b>CVE</b>	CVE-2021-41040
<b>State</b>	PUBLIC
<b>Assigner</b>	security@eclipse.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-02-01 12:15:00 UTC
<b>Updated</b>	2022-02-04 16:45:00 UTC
<b>Description</b>	In Eclipse Wakaama, ever since its inception until 2021-01-14, the CoAP parsing code does not properly sanitize network-r

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Eclipse</a>	<a href="#">Wakaama</a>	1.0	All	All	All

## References

Reference	Source	Link	Tags
Fix coap_parse_message() by rettichschnidi · Pull Request #640 · eclipse/wakaama · GitHub	CONFIRM	<a href="#">github.com</a>	
577968 – (CVE-2021-41040) Potential OOB reads in eclipse/wakaama may lead to DoS	CONFIRM	<a href="#">bugs.eclipse.org</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, and

No vendor comments have been submitted for this CVE.

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

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](#)**