



# CVE-2023-37788

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

## Summary

<b>CVE</b>	CVE-2023-37788
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-07-18 19:15:00 UTC
<b>Updated</b>	2023-07-27 04:05:00 UTC
<b>Description</b>	goproxy v1.1 was discovered to contain an issue which can lead to a Denial of service (DoS) via unspecified vectors.

## Risk And Classification

**Problem Types:** CWE-400

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Goproxy Project	Goproxy	1.1	All	All	All

## References

### Reference

- GitHub - elazarl/goproxy: An HTTP proxy library for Go
- goproxy v1.1 was discovered to contain an issue which can lead to Denial of Service (DoS) via unspecified vectors · Issue #502 · elazarl/goproxy
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[242374](#) Red Hat OpenShift Container Platform 4.14 Security Update (RHSA-2023:5009)

[770213](#) Red Hat OpenShift Container Platform 4.14 Security Update (RHSA-2023:5009)

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](#)**