



CVE-2023-26130

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2023-26130
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-30 05:15:00 UTC
Updated	2023-11-07 04:09:00 UTC
Description	Versions of the package yhirose/cpp-http lib before 0.12.4 are vulnerable to CRLF Injection when untrusted user input is use

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cpp-http lib Project	Cpp-http lib	All	All	All	All

References

Reference	Source	Link
Release Fix more CRLF injection problems · yhirose/cpp-http lib · GitHub	MISC	github.com
[SECURITY] Fedora 38 Update: cpp-http lib-0.12.5-1.fc38 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
CRLF Injection in cpp-http lib@v0.12.3 · GitHub	MISC	gist.github.com
CRLF Injection in yhirose/cpp-http lib CVE-2023-26130 Snyk	MISC	security.snyk.io
Fix more CRLF injection problems. · yhirose/cpp-http lib@5b397d4 · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[284078](#) Fedora Security Update for cpp (FEDORA-2023-0070b20b20)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)