



# cpp-httplib: HTTP Request Smuggling via Unconsumed GET Request Body

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

## Summary

<b>CVE</b>	CVE-2026-34441
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-31 22:16:19 UTC
<b>Updated</b>	2026-04-01 20:28:01 UTC
<b>Description</b>	cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to version 0.40.0, cpp-httplib is vuln

## Risk And Classification

**Primary CVSS:** v3.1 6.5 MEDIUM from nvd@nist.gov

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

**EPSS:** 0.000280000 probability, percentile 0.076440000 (date 2026-04-01)

**Problem Types:** CWE-444 | CWE-444 CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
3.1	security-advisories@github.com	Secondary	4.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	DECLARED	4.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

#### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yhirose	Cpp-httplib	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Yhirose	Cpp-httplib	affected < 0.40.0	Not specified

#### References

Reference	Source	Link	Tags
github.com/yhirose/cpp-httplib/releases/tag/v0.40.0	security-advisories@github.com	github.com	Product, Release
github.com/yhirose/cpp-httplib/security/advisories/GHSA-jv63-rm9j-6jwc	security-advisories@github.com	github.com	Exploit, Mitigation
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© 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](#)