VDB-355426 · CVE-2026-5638 · ISSUE 40

HERIKLYMA CPPWEBFRAMEWORK UP TO 3.1 PATH TRAVERSAL

CVSS Meta Temp Score

4.8

Current Exploit Price (≈)

$0-$5k

CTI Interest Score

2.76

Summary

A vulnerability categorized as critical has been discovered in HerikLyma CPPWebFramework up to 3.1. Impacted is an unknown function. Executing a manipulation can lead to path traversal. This vulnerability is handled as CVE-2026-5638. The attack can be executed remotely. Additionally, an exploit exists. The project was informed of the problem early through an issue report but has not responded yet.

Details

A vulnerability was found in HerikLyma CPPWebFramework up to 3.1. It has been declared as critical. This vulnerability affects an unknown functionality. The manipulation with an unknown input leads to a path traversal vulnerability. The CWE definition for the vulnerability is CWE-22. The product uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the product does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory. As an impact it is known to affect confidentiality.

The weakness was released by Matan Sandori as *40*. The advisory is available at github.com. This vulnerability was named CVE-2026-5638. The exploitation appears to be easy. The attack can be initiated remotely. No form of authentication is required for a successful exploitation. Technical details are unknown but a public exploit is available. This vulnerability is assigned to T1006 by the MITRE ATT&CK project.

It is possible to download the exploit at github.com. It is declared as proof-of-concept. The project was informed of the problem early through an issue report but has not responded yet.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

The vulnerability is also documented in the vulnerability database at EUVD (EUVD-2026-19205).

Product

Vendor

- HerikLyma

Name

- CPPWebFramework

Version

- 3.0
- 3.1

Website

- Product: https://github.com/HerikLyma/CPPWebFramework/

CPE 2.3

- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 5.3
VulDB Meta Temp Score: 4.8

VulDB Base Score: 5.3
VulDB Temp Score: 4.8
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Path traversal
CWE: CWE-22
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

04/05/2026		Advisory disclosed
04/05/2026	+0 days	VulDB entry created
04/06/2026	+1 days	VulDB entry last update

Sources

Product: github.com

Advisory: 40
Researcher: Matan Sandori
Status: Not defined

CVE: CVE-2026-5638 (🔒)
GCVE (CVE): GCVE-0-2026-5638
GCVE (VulDB): GCVE-100-355426
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/05/2026 10:26 PM
Updated: 04/06/2026 12:30 PM
Changes: 04/05/2026 10:26 PM (55), 04/06/2026 03:28 AM (1), 04/06/2026 12:30 PM (1)
Complete: 🔍
Submitter: MatanS
Committer: MatanS
Cache ID: 172:559:179

Submit

Accepted

- Submit #785952: HerikLyma CPPWebFramework <= 3.1 (HTTP Server Header) Relative Path Traversal (by MatanS)

Discussion

No comments yet. Languages: en.

Please log in to comment.