



EVERest: OCPP 1.6 heap corruption caused by lock-free insertion in event_queue

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

Summary

CVE	CVE-2026-26073
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-26 17:16:33 UTC
Updated	2026-03-30 21:04:21 UTC
Description	EVERest is an EV charging software stack. Versions prior to 2026.02.0 have a data race leading to possible `std::queue`/`st

Risk And Classification

Primary CVSS: v3.1 5.9 MEDIUM from security-advisories@github.com

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

EPSS: 0.000550000 probability, percentile 0.173260000 (date 2026-04-01)

Problem Types: CWE-122 | CWE-787 | CWE-122 CWE-122: Heap-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	DECLARED	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linuxfoundation	Everest	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	EVerest	Everest-core	affected < 2026.02.0	Not specified

References

Reference	Source	Link	Tags
github.com/EVerest/EVerest/security/advisories/GHSA-jf36-f4f9-7qc2	security-advisories@github.com	github.com	Vendor Advisory
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