EVerest has stack buffer overflow in ifreq.ifr_name when interface name exceeds IFNAMSIZ

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-23995
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-26 15:16:32 UTC
Updated	2026-03-31 13:49:39 UTC
Description	EVerest is an EV charging software stack. Prior to version 2026.02.0, stack-based buffer overflow in CAN interface initializa

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

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

EPSS: 0.000130000 probability, percentile 0.022000000 (date 2026-04-01)

Problem Types: CWE-121 | CWE-121 CWE-121: Stack-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	security-advisories@github.com	Secondary	8.4	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.4	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

vailability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/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-p47c-2jpr-mpwx	security-advisories@github.com	github.com	Exploit, Vendor A
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

No vendor comments have been submitted for this CVE.

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