Everon api.everon.io Improper Restriction of Excessive Authentication Attempts

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-24696
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-06 16:16:10 UTC
Updated	2026-05-06 14:34:58 UTC
Description	The WebSocket Application Programming Interface lacks restrictions on the number of authentication requests. This absen

Risk And Classification

Primary CVSS: v4.0 8.7 HIGH from ics-cert@hq.dhs.gov

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-307 | CWE-307 CWE-307 | CWE-307 CWE-307 Improper Restriction of Excessive Authentication Attempts

Version	Source	Type	Score	Severity	Vector
4.0	ics-cert@hq.dhs.gov	Secondary	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/
4.0	CNA	CVSS	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
3.1	ics-cert@hq.dhs.gov	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/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
Application	Everon	Api.everon.io	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms

CNA	Everon	Api.everon.io	affected All versions custom	Not specified

References

Reference	Source	Link	Tags
github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-06...	ics-cert@hq.dhs.gov	github.com	Product
www.cisa.gov/news-events/ics-advisories/icsa-26-062-08	ics-cert@hq.dhs.gov	www.cisa.gov	US Government Resc
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Khaled Sarieddine and Mohammad Ali Sayed reported this vulnerability to CISA. (en)

Additional Advisory Data

Workarounds

CNA: Everon shut down their platform on December 1st, 2025.

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