America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

EV2GO ev2go.io

Release Date: February 26, 2026 **Alert Code:** ICSA-26-057-04

RELATED TOPICS: INDUSTRIAL CONTROL SYSTEM VULNERABILITIES </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, INDUSTRIAL CONTROL SYSTEMS </topics/industrial-control-systems>

View CSAF <https://github.com/cisagov/csaf/blob/develop/csaf_files/ot/white/2026/icsa-26-057-04.json>

Summary

Successful exploitation of these vulnerabilities could allow attackers to impersonate charging stations, hijack sessions, suppress or misroute legitimate traffic to cause large-scale denial of service, and manipulate data sent to the backend.

The following versions of EV2GO ev2go.io are affected:

- ev2go.io vers:all/* (CVE-2026-24731, CVE-2026-25945, CVE-2026-20895, CVE-2026-22890)

CVSS	Vendor	Equipment	Vulnerabilities
v3 9.4	EV2GO	EV2GO ev2go.io	Missing Authentication for Critical Function, Improper Restriction of Excessive Authentication Attempts, Insufficient Session Expiration, Insufficiently Protected Credentials

Background

- **Critical Infrastructure Sectors:** Energy, Transportation Systems
- **Countries/Areas Deployed:** Worldwide
- **Company Headquarters Location:** United Kingdom

Vulnerabilities

Expand All +

CVE-2026-24731

CVE-2026-25945

CVE-2026-20895

CVE-2026-22890

Acknowledgments

- Khaled Sarieddine and Mohammad Ali Sayed reported these vulnerabilities to CISA

Legal Notice and Terms of Use

This product is provided subject to this Notification (https://www.cisa.gov/notification) and this Privacy & Use policy (https://www.cisa.gov/privacy-policy).

Recommended Practices

CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities, such as:

Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the Internet.

Locate control system networks and remote devices behind firewalls and isolating them from business networks.

When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as the connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on cisa.gov/ics. Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at cisa.gov/ics in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

No known public exploitation specifically targeting these vulnerabilities has been reported to CISA at this time.

Revision History

- **Initial Release Date:** 2026-02-26

Date	Revision	Summary
2026-02-26	1	Initial Publication

Legal Notice and Terms of Use

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Tags

Sector: Energy Sector </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector>, Transportation Systems Sector </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector>

Topics: Industrial Control System Vulnerabilities </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, Industrial Control Systems </topics/industrial-control-systems>

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Related Advisories

MAR 26, 2026 ■ ICS ADVISORY | ICSA-26-085-02

OpenCode Systems OC Messaging and USSD Gateway </news-events/ics-advisories/icsa-26-085-02>

MAR 26, 2026 ■ ICS ADVISORY | ICSA-26-085-03

PTC Windchill Product Lifecycle Management </news-events/ics-advisories/icsa-26-085-03>

MAR 26, 2026 ■ ICS ADVISORY | ICSA-26-085-01

WAGO GmbH & Co. KG Industrial Managed Switches </news-events/ics-advisories/icsa-26-085-01>

MAR 24, 2026 ■ ICS ADVISORY | ICSA-26-083-01

Pharos Controls Mosaic Show Controller </news-events/ics-advisories/icsa-26-083-01>

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </no-fear-act>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>

USA.gov <https://www.usa.gov/>

Website Feedback </forms/feedback>