America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

OpenPLC_V3 (Update A)

Last Revised: April 09, 2026 **Alert Code:** ICSA-25-345-10

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/2025/icsa-25-345-10.json>

Summary

Successful exploitation of these vulnerabilities could result in the alteration of PLC settings, upload of malicious programs, access to credentials, or bypass authentication.

The following versions of OpenPLC_V3 (Update A) are affected:

- OpenPLC_V3 vers:all/* (CVE-2025-13970, CVE-2026-28205, CVE-2026-35556, CVE-2026-35063)

CVSS	Vendor	Equipment	Vulnerabilities
v3 8.9	OpenPLC_V3	OpenPLC_V3 (Update A)	Cross-Site Request Forgery (CSRF), Initialization of a Resource with an Insecure Default, Plaintext Storage of a Password, Missing Authorization

Background

- **Critical Infrastructure Sectors:** Critical Manufacturing, Energy, Transportation Systems, Water and Wastewater
- **Countries/Areas Deployed:** Worldwide
- **Company Headquarters Location:** United States

Vulnerabilities

Expand All +

CVE-2025-13970 +

CVE-2026-28205 +

CVE-2026-35556 +

CVE-2026-35063 +

Acknowledgments

- Muhammad Ali and Anthony Marrongelli of University of Central Florida (UCF) reported vulnerability CVE-2025-13970 to CISA
- Shriyans Sudhi (ss0x00) of Rochester Institute of Technology (RIT) reported vulnerabilities CVE-2026-28205 and CVE-2026-35556 to CISA
- Arad Inbar, Nir Somech, Ben Grinberg, Daniel Lubel, Erez Cohen, and Adiel Sol of DREAM reported vulnerability CVE-2026-35063 to CISA

Legal Notice and Terms of Use

Recommended Practices

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability.

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 this vulnerability has been reported to CISA at this time. This vulnerability has a high attack complexity.

Revision History

- **Initial Release Date:** 2025-12-11

Date	Revision	Summary
2025-12-11	1	Initial Publication
2026-04-09	2	Update A - Update to mitigations and additional CVEs

Legal Notice and Terms of Use

Tags

Sector: Critical Manufacturing Sector </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/critical-manufacturing-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>, Water and Wastewater Systems </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/water-and-wastewater-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

APR 09, 2026 ■ ICS ADVISORY | ICSA-26-099-02

GPL Odorizers GPL750 </news-events/ics-advisories/icsa-26-099-02>

APR 09, 2026 ■ ICS ADVISORY | ICSA-26-099-01

Contemporary Controls BASC 20T </news-events/ics-advisories/icsa-26-099-01>

APR 07, 2026 ■ ICS ADVISORY | ICSA-26-097-01

Mitsubishi Electric GENESIS64 and ICONICS Suite products </news-events/ics-advisories/icsa-26-097-01>

APR 02, 2026 ■ ICS ADVISORY | ICSA-26-092-02

Yokogawa CENTUM VP </news-events/ics-advisories/icsa-26-092-02>

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>