Initialization of a resource with an insecure default in OpenPLC_V3

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

Summary

CVE	CVE-2026-28205
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 19:16:23 UTC
Updated	2026-04-13 15:02:27 UTC
Description	OpenPLC_V3 is vulnerable to an Initialization of a Resource with an Insecure Default vulnerability which could allow an atta

Risk And Classification

Primary CVSS: v4.0 9.2 CRITICAL from ics-cert@hq.dhs.gov

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:H/VA:H/SC:L/SI:H/SA:H/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

EPSS: 0.000870000 probability, percentile 0.249220000 (date 2026-04-15)

Problem Types: CWE-1188 | CWE-1188 CWE-1188 Initialization of a resource with an insecure default

Version	Source	Type	Score	Severity	Vector
4.0	ics-cert@hq.dhs.gov	Secondary	9.2	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:H/VA:H/SC:L/SI:H/SA:H/E:X
4.0	CNA	CVSS	9.2	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:H/VA:H/SC:L/SI:H/SA:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

None

Confidentiality

Low

Integrity

High

Availability

High

Sub Conf.

Low

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:H/VA:H/SC:L/SI:H/SA:H/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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OpenPLC V3	OpenPLC V3	affected All versions	Not specified

References

Reference	Source	Link	Tags
www.cisa.gov/news-events/ics-advisories/icsa-25-345-10	ics-cert@hq.dhs.gov	www.cisa.gov	
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: Shriyans Sudhi (ss0x00) from Rochester Institute of Technology (RIT) (en)

Additional Advisory Data

Workarounds

CNA: OpenPLC_v3 is now considered to be end of life. Users are recommended to upgrade to OpenPLC Runtime v4 (https://github.com/autonomy-logic/openplc-runtime).

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