

CVE-2021-26829

OpenPLC ScadaBR Cross-site Scripting Vulnerability

CISA KEV since Nov 28, 2025

Actively exploited

OpenPLC ScadaBR through 0.9.1 on Linux and through 1.12.4 on Windows allows stored XSS via system_settings.shtm.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 5.4 Medium · NVD	EPSS 0.480 98.9th percentile · FIRST	CISA DEADLINE Dec 19, 2025 CISA federal deadline · Overdue by 10 months
--	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.480 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 5.4	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle No patch reported by the connected remediation source

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. **CISA note:** This vulnerability could affect an open-source component, third-party library, protocol, or proprietary implementation that could be used by different products.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
scadabr	≤ 0.9.1 ≤ 1.12.4	after 0.9.1 · after 1.12.4	NVD
linux kernel	—	no fixed version listed	NVD
windows	—	no fixed version listed	NVD

Sources

Vendor guidance youtu.be/Xh6LPCiLMa8**Additional guidance** forescout.com/blog/anatomy-of-a-hacktivist-attack-russian-aligned-group-targets-otics/**github.com** github.com/SCADA-LTS/Scada-LTS/pull/3211**NVD** nvd.nist.gov/vuln/detail/CVE-2021-26829**CISA KEV** cisa.gov/known-exploited-vulnerabilities-catalog**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2021-13614**Current data** evulnable.com/vulnerability-management/cve/CVE-2021-26829

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.