



CVE-2021-26828

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-26828
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-11 12:15:00 UTC
Updated	2021-06-21 18:47:00 UTC
Description	OpenPLC ScadaBR through 0.9.1 on Linux and through 1.12.4 on Windows allows remote authenticated users to upload a

Risk And Classification

EPSS: 0.800170000 probability, percentile 0.990980000 (date 2026-04-01)

CISA KEV: Listed on 2025-12-03; due 2025-12-24; ransomware use Unknown

Problem Types: CWE-434

CISA Known Exploited Vulnerability

Vendor	OpenPLC
Product	ScadaBR
Name	OpenPLC ScadaBR Unrestricted Upload of File with Dangerous Type Vulnerability
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.
Notes	This vulnerability could affect an open-source component, third-party library, protocol, or proprietary implementation that could be used by different products. For more information, please see: https://github.com/SCADA-LTS/Scada-LTS/pull/2174 ; https://nvd.nist.gov/vuln/detail/CVE-2021-26828

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openplcproject	Scadabr	All	All	All	All
Application	Openplcproject	Scadabr	All	All	All	All

References

Reference	Source	Link
[REPORT] Falhas de segurança em versões do ScadaBR - ScadaBR - Geral - ScadaBR	MISC	forum.sca
CVE-2021-26828 - ScadaBR - Geral - ScadaBR	MISC	forum.sca

ScadaBR 1.0 / 1.1 CE Linux Shell Upload ≈ Packet Storm	MISC	packetsto
ScadaBR CE 1.12.4 - Remote Code Execution via Arbitrary File Upload (Authenticated) - Windows 7 x64 - YouTube	MISC	youtu.be
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa



No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)