

Posted Date: 2025/12/03

[Vulnerability Alert] CISA Adds 1 Known Exploited Vulnerability to KEV Catalog (2025/11/24-2025/11/30)(CVE-2021-26829)

- Subject: [Vulnerability Alert] CISA Adds 1 Known Exploited Vulnerability to KEV Catalog (2025/11/24-2025/11/30)(CVE-2021-26829)
- Content:
 - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center Security Alert TWCERTCC-200-202512-00000001
 - [CVE-2021-26829] OpenPLC ScadaBR Cross-site Scripting Vulnerability (CVSS v3.1: 5.4)
 - [Exploited by Ransomware: Unknown] OpenPLC ScadaBR has a Cross-site Scripting vulnerability that can be triggered via the system_settings.shtm file.
- Affected Platforms:
 - OpenPLC ScadaBR Linux versions up to and including 0.9.1
 - OpenPLC ScadaBR Windows versions up to and including 1.12.4
- Recommended Measures:
 - Update the corresponding products to the following versions (or later):
 - OpenPLC ScadaBR Linux versions later than 0.9.1 (exclusive)
 - OpenPLC ScadaBR Windows versions later than 1.12.4 (exclusive)
- References:
 1. <https://www.twcert.org.tw/tw/cp-132-10519-5d666-1.html>

Computer and Communications Center
Network Systems Group

From:
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20251203_02

Last update: 2025/12/03 11:44