INTRUVENT

VULNERABILITY ADVISORY

OpenPLC ScadaBR

CVE-2021-26828 (RCE) & CVE-2021-26829 (XSS) - ICS/SCADA Vulnerabilities Under Active Hacktivist Exploitation

Highest CVSS 8.8 (High)
Classification TLP:CLEAR
Published December 7, 2025
Exploitation Active - CISA KEV

Intruvent Technologies
INT-VA-2025-OPENPLC-SCADABR-v1.0

1 Executive Summary

Critical Warning - ICS/SCADA Systems Under Active Attack

- Both CVEs added to CISA Known Exploited Vulnerabilities catalog
- Active exploitation by TwoNet pro-Russian hacktivist group
- Targets include water treatment facilities and critical infrastructure
- CISA deadlines: December 19, 2025 (XSS) and December 24, 2025 (RCE)

8.8 CVE-2021-26828
Arbitrary File Upload / RCE

Unrestricted file upload in view_edit.shtm allows authenticated attackers to upload malicious JSP files, achieving remote code execution on the ScadaBR Tomcat server.

`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H`

5.4 CVE-2021-26829
Stored Cross-Site Scripting

Stored XSS vulnerability in system_settings.shtm allows authenticated attackers to inject malicious JavaScript that executes when other users view the settings page.

`CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N`

Active Exploitation | CISA KEV Listed | ICS/SCADA Target | Public PoC Available

OpenPLC ScadaBR, an open-source SCADA Human-Machine Interface (HMI) system, contains two critical vulnerabilities that are being actively exploited by the TwoNet hacktivist group. In September 2025, Forescout Vedere Labs documented attacks against water treatment facility honeypots where attackers combined default credential access with these vulnerabilities to deploy web shells and compromise industrial control systems.

The addition of both CVEs to the CISA Known Exploited Vulnerabilities (KEV) catalog in late 2025—despite the vulnerabilities being patched in June 2021—highlights the persistent risk posed by unpatched OT/ICS systems. Organizations running ScadaBR in production environments must prioritize immediate remediation.

Vulnerability Timeline

June 2021	Sep 2025	Nov 28, 2025	Dec 3, 2025
Patches Released	TwoNet Attacks	CISA KEV (XSS)	CISA KEV (RCE)

2 Threat Actor: TwoNet

TwoNet Hacktivist Group Profile

ALIGNMENT	FIRST OBSERVED	PRIMARY PLATFORM
Pro-Russian Hacktivist	January 2025	Telegram
INITIAL FOCUS	**EVOLVED ACTIVITIES**	**SKILL LEVEL**
DDoS (MegaMedusa Machine)	ICS targeting, Doxxing, RaaS	Low-to-Moderate

TwoNet emerged in January 2025 as a pro-Russian hacktivist collective operating primarily through Telegram. Initially focused on DDoS attacks using their "MegaMedusa Machine" malware, the group has evolved to target industrial control systems, particularly water treatment facilities.

According to Forescout Vedere Labs research published in October 2025, TwoNet attacked a water treatment honeypot system in September 2025. The attack demonstrated a low-sophistication approach: leveraging default credentials combined with publicly available exploits for CVE-2021-26828 to deploy Java-based web shells.

Claimed Affiliations

- **CyberTroops** - Pro-Russian hacktivist collective
- **OverFlame** - Affiliated threat group

Attack Methodology

1. Scan for exposed ScadaBR instances (typically port 8080)
2. Attempt authentication with default credentials (admin/admin)
3. Exploit CVE-2021-26828 to upload malicious JSP web shell
4. Establish persistent access to SCADA/HMI system
5. Potential manipulation of connected OT processes

3 Affected Products

ScadaBR (Linux)

- ✗ Version 0.9.1 and earlier - Vulnerable
- ✔ Post-June 2021 releases - Fixed

ScadaBR (Windows)

- ✗ Version 1.12.4 and earlier - Vulnerable
- ✔ Post-June 2021 releases - Fixed

What is ScadaBR?
ScadaBR is an open-source SCADA (Supervisory Control and Data Acquisition) system that provides Human-Machine Interface (HMI) capabilities for industrial control systems. It is commonly deployed as part of the OpenPLC software stack to provide a graphical interface for monitoring and controlling PLCs (Programmable Logic Controllers).

ScadaBR runs as a Java web application on Apache Tomcat and is used in:

- Water treatment and distribution facilities
- Industrial manufacturing automation
- Building automation systems
- Educational and research environments
- Small-scale OT deployments

4 Technical Analysis

CVE-2021-26828: Arbitrary File Upload / Remote Code Execution

Vulnerability Description
The `view_edit.shtm` endpoint in ScadaBR allows authenticated users to create and modify graphical views for HMI displays. This functionality includes uploading background images for views. However, the upload mechanism fails to properly validate file types, allowing attackers to upload arbitrary files with dangerous extensions such as `.jsp`.

Root Cause
CWE-434: Unrestricted Upload of File with Dangerous Type

The application does not verify that uploaded files match expected image types (JPEG, PNG, GIF). An attacker can upload a JSP web shell disguised as or named with any extension, which is then stored in a web-accessible directory and can be executed directly by the Tomcat application server.

CVE-2021-26828 Exploitation Chain

Phase 1
Authentication
Attacker authenticates to ScadaBR using default or compromised credentials

↓

Phase 2
Access View Editor
Navigate to /ScadaBR/view_edit.shtm to access the graphical view editor

↓

Phase 3
Upload Malicious JSP
Upload JSP web shell via background image upload functionality

↓

Phase 4
Remote Code Execution
Access uploaded JSP file directly to execute arbitrary commands on Tomcat server

Attack Vector Details

```
Vulnerable Endpoint
POST /ScadaBR/view_edit.shtm HTTP/1.1
Host: target:8080
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary...

------WebKitFormBoundary...
Content-Disposition: form-data; name="backgroundImageMP"; filename="shell.jsp"
Content-Type: image/jpeg

<%@ page import="java.io.*" %>
<% /* JSP web shell payload */ %>
------WebKitFormBoundary...--
```

CVE-2021-26829: Stored Cross-Site Scripting

Vulnerability Description
The `system_settings.shtm` endpoint in ScadaBR is vulnerable to stored cross-site scripting (XSS). An authenticated attacker can inject malicious JavaScript into system settings fields, which is then executed in the browsers of other users who view the settings page.

Root Cause
CWE-79: Improper Neutralization of Input During Web Page Generation

User-supplied input in system settings fields is not properly sanitized or encoded before being rendered in the web interface. This allows injection of script tags or event handlers that execute arbitrary JavaScript.

Impact

- Session hijacking of other ScadaBR users
- Credential theft via phishing overlays
- Privilege escalation if administrator sessions are compromised
- Chaining with CVE-2021-26828 for automated exploitation

5 Remediation

CRITICAL PRIORITY CISA Deadline: December 19, 2025 (XSS) | December 24, 2025 (RCE)

Patching Guidance

1. **Upgrade ScadaBR** to the latest version available from the OpenPLC project
2. **Verify patch status** - Both vulnerabilities were patched in June 2021 releases
3. **Test in staging** before deploying to production OT environments
4. **Coordinate with operations** to schedule maintenance windows for critical systems

IMMEDIATE MITIGATIONS (IF PATCHING IS DELAYED)

- **Change default credentials** - Replace admin/admin with strong unique passwords
- **Network isolation** - Remove ScadaBR from internet-accessible networks
- **Access restrictions** - Limit ScadaBR access to authorized IP ranges only
- **WAF rules** - Block JSP file uploads and requests containing script tags
- **Monitor uploads** - Alert on any file uploads via view_edit.shtm endpoint

NETWORK SEGMENTATION REQUIREMENTS

ScadaBR and OpenPLC systems should **never** be directly accessible from the internet. Implement proper OT network segmentation:

- Place SCADA systems in dedicated OT network zones
- Use jump hosts or VPNs for remote access
- Implement allowlist-based firewall rules
- Deploy network monitoring at IT/OT boundaries

6 Detection

Indicators of Exploitation

Web Server Logs - CVE-2021-26828

```
Tomcat Access Log Patterns
# JSP file upload attempts
POST /ScadaBR/view_edit.shtm .*\.jsp

# Web shell access patterns
GET /ScadaBR/uploads/.*\.jsp
GET /ScadaBR/.*\.jsp HTTP.* (excluding known legitimate JSP files)

# Command execution indicators in web shell requests
\?cmd=|\?c=|\?command=
```

Web Server Logs - CVE-2021-26829

```
XSS Attack Patterns
# Script injection in system settings
POST /ScadaBR/system_settings.shtm .*<script|javascript:|onerror=|onload=
```

File System Indicators

- Unexpected `.jsp` files in ScadaBR directories
- Recently modified files in `/ScadaBR/uploads/`
- Web shell signatures (cmd.jsp, shell.jsp, etc.)

Detection Rules

```
Sigma Rule - ScadaBR File Upload Exploitation
title: ScadaBR Malicious File Upload (CVE-2021-26828)
status: experimental
description: Detects potential exploitation of CVE-2021-26828 via JSP file upload
logsource:
    category: webserver
    product: tomcat
detection:
    selection:
        cs-method: POST
        cs-uri-stem|contains: '/ScadaBR/view_edit.shtm'
    filter_jsp:
        cs-uri-query|contains: '.jsp'
    condition: selection or (selection and filter_jsp)
falsepositives:
    - Legitimate administrative activity
level: high
tags:
    - attack.initial_access
    - attack.t1190
    - cve.2021.26828
```

```
Snort/Suricata Rule - Web Shell Upload
alert http any any -> any any (msg:"ET EXPLOIT ScadaBR JSP Upload Attempt CVE-2021-26828";
  flow:established,to_server;
  content:"POST"; http_method;
  content:"/ScadaBR/view_edit.shtm"; http_uri;
  content:".jsp"; http_client_body;
  classtype:web-application-attack;
  sid:1000001; rev:1;)
```

A Appendix: Indicators of Compromise

IOC Sourcing
Indicators sourced from Forescout Vedere Labs TwoNet attack analysis (October 2025). IOC currency verified: December 7, 2025.

Network Indicators - TwoNet Infrastructure

Indicator	Type	Context	Confidence
45.157.234[.]199	IPv4	TwoNet attack infrastructure - water treatment honeypot attack (AS58212)	High
45.14.247[.]87	IPv4	TwoNet attack infrastructure	High

Vulnerable Endpoints

Endpoint	Method	CVE	Exploit Context
/ScadaBR/view_edit.shtm	POST	CVE-2021-26828	JSP web shell upload via background image
/ScadaBR/system_settings.shtm	POST	CVE-2021-26829	JavaScript injection in settings fields

File Indicators

Indicator	Type	Context
*.jsp in upload directories	File Extension	Web shell uploads - should not exist in image directories
cmd.jsp, shell.jsp, upload.jsp	Filename	Common web shell naming patterns

User Agent

User Agent	Context
python-requests/2.28.1	Automated exploitation tool - indicates scripted attacks

B Appendix: References

[1] National Vulnerability Database - CVE-2021-26828
https://nvd.nist.gov/vuln/detail/CVE-2021-26828

[2] National Vulnerability Database - CVE-2021-26829
https://nvd.nist.gov/vuln/detail/CVE-2021-26829

[3] Forescout Vedere Labs - "Anatomy of a Hacktivist Attack: Russian-Aligned Group Targets OT/ICS"
https://www.forescout.com/blog/anatomy-of-a-hacktivist-attack-russian-aligned-group-targets-otics/

[4] CISA Known Exploited Vulnerabilities Catalog
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[5] The Hacker News - "CISA Adds Actively Exploited XSS Bug to KEV"
https://thehackernews.com/2025/11/cisa-adds-actively-exploited-xss-bug.html

[6] SecurityWeek - "CISA Warns of ScadaBR Vulnerability After Hacktivist ICS Attack"
https://www.securityweek.com/cisa-warns-of-scadabr-vulnerability-after-hacktivist-ics-attack/

[7] Industrial Cyber - "OpenPLC ScadaBR Added to CISA's Known Exploited List After Confirmed Attacks"
https://industrialcyber.co/industrial-cyber-attacks/openplc-scadabr-added-to-cisas-known-exploited-list-after-confirmed-attacks/

[8] Security Affairs - "U.S. CISA Adds OpenPLC ScadaBR Flaw to KEV Catalog"
https://securityaffairs.com/185185/security/u-s-cisa-adds-an-openplc-scadabr-flaw-to-its-known-exploited-vulnerabilities-catalog.html