Smarttech
YOUR 24/7 SECURITY PARTNER

# Multiple Vulnerabilities in Industrial Control Systems - 25th March 2026

| | |
|---|---|
| **Document ID** | SMA-Threat Report |
| **Document status** | ISSUED |
| **Issue Number** | 42 |
| **Authors** | Gabriel Gheorghiu< gabriel.gheorghiu@smarttech247.com > |
| **Verified by** | Alin Curcan < alin.curcan@smarttech247.com > |
| **Last modified** | 2026-03-25 |
| **Issue Date** | 2026-03-25 |

**Threat Reports** are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

## Overview

Multiple vulnerabilities have been identified in the following ICS products: Pharos Controls Mosaic Show Controller, Schneider Electric EcoStruxure Foxboro DCS and the Schneider Electric Plant iT/Brewmaxx. Successful exploitation of these vulnerabilities could enable privilege escalation, unauthenticated root-level command execution, insecure deserialization, and ultimately lead to remote code execution, loss of confidentiality, integrity, and availability, and unauthorized control of affected systems.

## Pharos Controls Mosaic Show Controller

### Summary

Successful exploitation of this vulnerability could allow an unauthenticated attacker to execute arbitrary commands with root privileges. The following versions of Pharos Controls Mosaic Show Controller are affected: **Mosaic Show Controller Firmware 2.15.3**

- **CVSS v.3 9.8**
- **Vendor:** Pharos Controls
- **Equipment:** Pharos Controls Mosaic Show Controller
- **Vulnerabilities:** Missing Authentication for Critical Function

### Vulnerabilities

| CVE ID | Base Severity | Description |
|---|---|---|
| **CVE-2026-2417** | Critical | A Missing Authentication for Critical Function vulnerability in Pharos Controls Mosaic Show Controller firmware version 2.15.3 could allow an unauthenticated attacker to bypass authentication and execute arbitrary commands with root privileges. |

### Remediations

- Pharos Controls recommends that users upgrade Mosaic Show Controller to version 2.16 or later.

## Schneider Electric EcoStruxure Foxboro DCS

**Summary**
Successful exploitation of this vulnerability could lead to deserialization of untrusted data, resulting in loss of confidentiality, integrity, and potential remote code execution on affected systems. The following versions of Schneider Electric EcoStruxure Foxboro DCS are affected:
**EcoStruxure Foxboro DCS versions prior to CS8.1**

- **CVSS v3 6.5**
- **Vendor:** Schneider Electric.
- **Equipment:** Schneider Electric EcoStruxure Foxboro DCS.
- **Vulnerabilities:** Deserialization of Untrusted Data.

**Vulnerabilities**

| CVE ID | Base Severity | Description |
|---|---|---|
| **CVE-2026-1286** | Medium | A deserialization of untrusted data vulnerability exists that could lead to loss of confidentiality, integrity and potential remote code execution on workstation when an admin authenticated user opens a malicious project file. |

**Remediations:**

**Vendor fix:** A fix is available in version CS 8.1 of the EcoStruxure Foxboro DCS Control Software, which requires updated licensing and a system reboot. Depending on the current setup, upgrades may be performed without interrupting production, and coordination with Schneider Electric support is recommended.

**Mitigation:** If the patch is not applied, risk can be reduced by only using trusted data sources, validating incoming files, and rejecting suspicious or malformed data. Additional measures include securing communications, avoiding removable media, limiting administrative privileges, and isolating DCS systems to minimize exposure.

## Schneider Electric Plant iT/Brewmaxx

**Summary**
Successful exploitation of these vulnerabilities could risk privilege escalation, which could result in remote code execution. The following versions of Schneider Electric Plant iT/Brewmaxx are affected: **Plant iT/Brewmaxx 9.60 and above**

- **CVSS v3 9.9**
- **Vendor:** Schneider Electric
- **Equipment:** Schneider Electric Plant iT/Brewmaxx
- **Vulnerabilities:** Use After Free, Integer Overflow or Wraparound, Improper Control of Generation of Code ('Code Injection')

**Vulnerabilities**

| CVE ID | Base Severity | Description |
|---|---|---|
| **CVE-2025-49844** | Critical | The affected product uses Redis, an open-source, in-memory database. Versions 8.2.1 and below allow an authenticated user to use a specially crafted Lua script to manipulate the garbage collector, trigger a use-after-free, and potentially lead to remote code execution. |
| **CVE-2025-** | High | The affected product uses Redis, an open-source, in-memory database. |

| | | |
|---|---|---|
| **46817** | | Versions 8.2.1 and below allow an authenticated user to use a specially crafted Lua script to cause an integer overflow and potentially lead to remote code execution |
| **CVE-2025-46818** | Medium | The affected product uses Redis, an open-source, in-memory database. Versions 8.2.1 and below allow an authenticated user to use a specially crafted Lua script to manipulate different LUA objects and potentially run their own code in the context of another user. |
| **CVE-2025-46819** | Medium | The affected product uses Redis, an open-source, in-memory database. Versions 8.2.1 and below allow an authenticated user to use a specially crafted LUA script to read out-of-bound data or crash the server and subsequent denial of service |

**Remediations**

- Install ProLeiT-2025-001 patch via ProLeiT Support.
- Disable Redis eval commands on application servers, VisuHub, and workstations after patching.
- Enforce secure Redis configuration templates as specified in the patch documentation.
- Restart all affected systems after applying the patch.
- Isolate control and safety systems behind firewalls and separate them from business networks.
- Minimize network exposure and ensure systems are not accessible from the internet.
- Use secure remote access methods (e.g., VPNs) and keep them up to date.
- Restrict physical access to control systems and related components.
- Keep controllers in locked cabinets and avoid “Program” mode when not required.
- Limit administrative and engineering privileges to essential personnel only
- Ensure all operations are performed with least privilege access.
- Only use trusted data sources and validate incoming files.
- Scan removable media (USBs, CDs, etc.) before use.
- Avoid using mobile devices that have connected to untrusted networks.

References

https://www.cisa.gov/news-events/ics-advisories/icsa-26-083-01
https://www.cisa.gov/news-events/ics-advisories/icsa-26-083-02
https://www.cisa.gov/news-events/ics-advisories/icsa-26-083-03

CVEs

CVE-2026-2417
CVE-2026-1286
CVE-2025-49844
CVE-2025-46817
CVE-2025-46818
CVE-2025-46819

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com