Smarttech
YOUR 24/7 SECURITY PARTNER

Multiple Vulnerabilities in Industrial Control Systems - 14th August 2026

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	137
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-08-14
Issue Date	2026-08-13

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-connected products: **Johnson Controls Metasys, Flow Neuroscience FL-100, Siemens LOGO! Soft Comfort, Siemens Solid Edge, Siemens Simcenter Femap, Siemens Parasolid, Siemens Siveillance Video, Siemens Desigo DXR and PXC Controllers, Siemens License Server (SLS), ANDRITZ HIPASE-250 and 250 SCALA, Hitachi Energy APM Edge Product, Johnson Controls Inc. Airwall, Haiwell IoT Cloud HMI Gateway,** and **AVEVA Enterprise SCADA**. Successful exploitation of the vulnerabilities addressed in these advisories may result in unauthorized access, remote code execution, privilege escalation, information disclosure, cross-site scripting, OS command injection, data manipulation, denial-of-service and compromise the confidentiality, integrity and availability of affected systems.

Johnson Controls Metasys

Summary

Successful exploitation of this vulnerability could allow a low-privilege user or attacker to inject a persistent malicious payload via a crafted URL that executes in the context of other users' sessions, including administrators, potentially leading to session hijacking and unauthorized access.

The following versions of Johnson Controls Metasys are affected:

- **Metasys 12 vers:all/* (CVE-2026-34491)**
- **Metasys 13 vers:all/* (CVE-2026-34491)**
- **Metasys 14**
- **Metasys 15**

- **CVSS v3 8**
- **Vendor:** Johnson Controls Inc
- **Equipment:** Johnson Controls Metasys
- **Vulnerabilities:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-34491	High	A low-privilege user can inject a malicious XSS payload into the

		Metasys UI via a crafted URL. The payload persists across logins and executes in the browser context of other users, including administrators.

Remediation:

- Johnson Controls recommends users to apply the latest available patches for affected Metasys versions
- Metasys 16.0: Not impacted, fixed prior to release
- Metasys 15.0: Patch released 2026-03-25
- Metasys 14.1.5: Forecast release 2026-07-15
- Metasys 13: End of support, update to later version
- Metasys 12: End of support, update to later version
- Metasys 11 & prior: Not affected (vulnerability introduced at version 12)
- Upgrade to Metasys version 16.0 or apply the latest available patch for your version (15.0.1 or 14.1.5 when available)
- Restrict network access to the Metasys UI to trusted networks and users only; do not expose the interface directly to the internet
- Implement network segmentation to isolate building automation systems from the corporate IT network
- Enforce least-privilege access controls – limit user accounts to the minimum permissions necessary
- Implement Content Security Policy (CSP) headers and other HTTP security headers where possible at the network/proxy level
- Monitor for suspicious URL patterns and unexpected script execution in Metasys UI access logs
- Use a web application firewall (WAF) in front of the Metasys UI to detect and block common XSS payloads
- Educate users to avoid clicking on untrusted or unexpected links that target the Metasys UI

Flow Neuroscience FL-100

Summary

Successful exploitation of this vulnerability could allow an attacker within Bluetooth range to manipulate brain stimulation parameters and override safety limits.

The following versions of Flow Neuroscience FL-100 are affected:

- **Flow Neuroscience FL-100**
- **Halo Neuroscience FL-100**

- **CVSS v3 8.1**
- **Vendor:** Flow Neuroscience
- **Equipment:** Flow Neuroscience FL-100
- **Vulnerabilities:** Use of Hard-coded Credentials

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-18164	High	An undocumented hard-coded credential, shared by all device units, is authorized to bypass authentication. This allows an attacker within Bluetooth range to arbitrarilymanipulate brain stimulation parameters and state.

Remediation:

- Users are encouraged to install the latest firmware updates provided by Flow Neuroscience via the Flow app.

Siemens LOGO! Soft Comfort

Summary

Siemens LOGO! Soft Comfort contains multiple vulnerabilities in its project-file encryption and password handling mechanisms. A local attacker could exploit these vulnerabilities to extract the master key, allowing them to decrypt project data or remove project passwords. The lack of password salting enables offline dictionary or brute-force attacks against the password hashes. Successful exploitation could result in unauthorized access to, or modification of, sensitive project logic and configurations. Siemens has released a new version for LOGO! Soft Comfort and recommends to update to the latest version.

The following versions of Siemens LOGO! Soft Comfort are affected:

- **LOGO! Soft Comfort vers:intdot/<9 (CVE-2026-57262, CVE-2026-57263)**

- **CVSS v3 6.8**
- **Vendor:** Siemens
- **Equipment:** Siemens LOGO! Soft Comfort
- **Vulnerabilities:** Use of Hard-coded Cryptographic Key, Use of a One-Way Hash without a Salt

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-57262	Medium	Affected products use a static, hardcoded AES master key to encrypt project files. This could allow a local attacker to extract the master key from the application files or memory and use it to decrypt project files or remove project passwords entirely without knowing the actual user-defined password.
CVE-2026-57263	Medium	The project password feature in the affected products stores the password as an unsalted SHA-256 hash. This could allow an attacker who has obtained the project file to perform efficient offline dictionary or brute-force attacks against the unsalted hash.

Remediation:

- Update to V9 or later version

Note: A hardware upgrade to LOGO! V9 BM or later is also required to avoid compatibility mode, in which the vulnerabilities addressed by this advisory remain present.

Siemens Solid Edge

Summary

Solid Edge is affected by multiple file parsing vulnerabilities that could be triggered when the application reads specially crafted files in PAR, PSM or DFT format. This could allow an

attacker to crash the application or execute arbitrary code. Siemens has released new versions for the affected products and recommends to update to the latest versions.

The following versions of Siemens Solid Edge are affected:

- **Solid Edge SE2025 vers:intdot/<225.0.15 (CVE-2026-50058, CVE-2026-50059, CVE-2026-50060, CVE-2026-50061, CVE-2026-50062, CVE-2026-50063, CVE-2026-50064)**
- **Solid Edge SE2026 vers:intdot/<226.0.7 (CVE-2026-50058, CVE-2026-50059, CVE-2026-50060, CVE-2026-50061, CVE-2026-50062, CVE-2026-50063, CVE-2026-50064)**

- **CVSS v3 7.8**
- **Vendor:** Siemens
- **Equipment:** Siemens Solid Edge
- **Vulnerabilities:** Out-of-bounds Read, Out-of-bounds Write, Use After Free

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-50058	High	The affected applications contain an out of bounds read vulnerability while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process.
CVE-2026-50059	High	The affected applications contain an out of bounds write vulnerability while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process.
CVE-2026-50060	High	The affected applications contain a use-after-free vulnerability that could be triggered while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process.
CVE-2026-50061	High	The affected applications contain a use-after-free vulnerability that could be triggered while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process.
CVE-2026-50062	High	The affected applications contain an out of bounds read vulnerability while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.
CVE-2026-50063	High	The affected applications contain an out of bounds read vulnerability while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.
CVE-2026-50064	High	The affected applications contain an out of bounds write vulnerability while parsing specially crafted PSM files. This could allow an attacker to execute code in the context of the current process.

Remediation:

- Update to V225.0 Update 15 or later version
- Update to V226.0 Update 7 or later version

Siemens Simcenter Femap

Summary

Simcenter Femap contains two file parsing vulnerabilities that could be triggered when the application reads files in BMP file format. If a user is tricked to open a malicious file with the affected application, this could lead the application to crash or potentially lead to arbitrary code execution. Siemens has released a new version for Simcenter Femap and recommends to update to the latest version.

The following versions of Siemens Simcenter Femap are affected:

- **Simcenter Femap vers:intdot/<2606.0001 (CVE-2026-59700, CVE-2026-59701)**

- **CVSS v3 7.8**
- **Vendor:** Siemens
- **Equipment:** Siemens Simcenter Femap
- **Vulnerabilities:** Out-of-bounds Read

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-59700	High	The affected applications contains an out of bounds read vulnerability while parsing specially crafted BMP files. This could allow an attacker to execute code in the context of the current process.
CVE-2026-59701	High	The affected applications contains an out of bounds read vulnerability while parsing specially crafted BMP files. This could allow an attacker to execute code in the context of the current process.

Remediation:

- Update to V2606.0001 or later version

Siemens Parasolid

Summary

Parasolid is affected by an out of bounds read vulnerability that could be triggered when the application reads files in X_T format. This could allow an attacker to crash the application or execute arbitrary code. Siemens has released new versions for the affected products and recommends to update to the latest versions.

The following versions of Siemens Parasolid are affected:

- **Parasolid V38.0 vers:intdot/<38.0.235 (CVE-2026-64629)**
- **Parasolid V38.1 vers:intdot/<38.1.230 (CVE-2026-64629)**

- **CVSS v3 7.8**
- **Vendor:** Siemens
- **Equipment:** Siemens Parasolid
- **Vulnerabilities:** Out-of-bounds Read

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-64629	High	The affected applications contains an out of bounds read vulnerability while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.

Remediation:

- Update to V38.0.235 or later version
- Update to V38.1.230 or later version

Siemens Siveillance Video

Summary

Siveillance Video Management Servers contains a vulnerability that could allow a Remote Code Execution attack. Siemens has released new versions for the affected products and recommends to update to the latest versions.

The following versions of Siemens Siveillance Video are affected:

- **Siveillance Video V2023 R3 vers:intdot/<23.3.27 (CVE-2026-3014)**
- **Siveillance Video V2024 R1 vers:intdot/<24.1.16 (CVE-2026-3014)**
- **Siveillance Video V2025 vers:intdot/<25.1.15 (CVE-2026-3014)**

- **CVSS v3 9.1**
- **Vendor:** Siemens
- **Equipment:** Siemens Siveillance Video
- **Vulnerabilities:** Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-3014	Critical	Milestone has released a new version of XProtect® (and several cumulative patch updates) which fix security vulnerability in Management Server API. The vulnerability causes users with edit permissions to the Management Server to be able to execute arbitrary code in context of the Management Server Service.

Remediation:

- Update to V23.3 HotfixRev27 or later version
- Update to V24.1 HotfixRev16 or later version
- Update to V25.1 HotfixRev15 or later version

Siemens Desigo DXR and PXC Controllers

Summary

A vulnerability in Desigo DXR and PXC controllers has been identified that could allow an

attacker to cause denial of service conditions by sending malformed BACnet packets. Recovery requires a device reset or reboot to restore normal functionality. Siemens has released new versions for the affected products and recommends to update to the latest versions.

The following versions of Siemens Desigo DXR and PXC Controllers are affected:

- **Desigo DXR2 vers:intdot/<01.21.233.16-7862 (CVE-2026-59693)**
- **Desigo PXC3 vers:intdot/<01.21.233.16-7862 (CVE-2026-59693)**
- **Desigo PXC4 vers:intdot/<02.21.194.36-2715 (CVE-2026-59693)**
- **Desigo PXC5.E003 vers:intdot/<02.21.194.36-2715 (CVE-2026-59693)**
- **Desigo PXC5.E24 vers:intdot/<02.21.194.36-2715 (CVE-2026-59693)**
- **Desigo PXC7 vers:intdot/<02.21.194.36-2715 (CVE-2026-59693)**

- **CVSS v3 4.3**
- **Vendor:** Siemens
- **Equipment:** Siemens Desigo DXR and PXC Controllers
- **Vulnerabilities:** Improper Check for Unusual or Exceptional Conditions

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-59693	Medium	The affected devices are vulnerable to a denial-of-service (DoS) vulnerability. An attacker can exploit this issue by sending a malformed BACnet packet, causing the device to stop responding to BACnet queries. Recovery requires a device reset or reboot to restore normal functionality.

Remediation:

- Update to V01.21.233.16-7862 or later version Please contact your local Siemens office for additional support in obtaining the update.
- Update to V02.21.194.36-2715 or later version Please contact your local Siemens office for additional support in obtaining the update.

Siemens License Server (SLS)

Summary

Siemens License Server is affected by multiple vulnerabilities which could allow an attacker to elevate its privileges and read arbitrary files on the system. Siemens has released a new version for Siemens License Server (SLS) and recommends to update to the latest version.

The following versions of Siemens License Server (SLS) are affected:

- **Siemens License Server (SLS) vers:intdot/<5.1, vers:intdot/<5.3 (CVE-2026-69108, CVE-2026-69109)**

- **CVSS v3 7.5**
- **Vendor:** Siemens
- **Equipment:** Siemens License Server (SLS)
- **Vulnerabilities:** Incorrect Permission Assignment for Critical Resource, Path Traversal

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-69108	Medium	The affected application is vulnerable to a local privilege escalation due to an insecure sudoers policy. This could allow an attacker to execute arbitrary commands and plant malicious files as root, leading to full system compromise.
CVE-2026-69109	High	The affected application is vulnerable to a path traversal vulnerability due to lack of sanitization of user input. This could allow a remote attacker to access arbitrary files on the application.

Remediation:

- Update to V5.1 or later version
- Update to V5.3 or later version

ANDRITZ HIPASE-250 and 250 SCALA

Summary

Successful exploitation of these vulnerabilities could allow an attacker to read data from the device or gain access to affected workstations.

The following versions of ANDRITZ HIPASE-250 and 250 SCALA are affected:

- **HIPASE-250 <=7.20 (CVE-2026-65309, CVE-2026-65310, CVE-2026-65311, CVE-2026-65313)**
- **250 SCALA <=7.20 (CVE-2026-65309, CVE-2026-65310, CVE-2026-65311, CVE-2026-65313)**

- **CVSS v3 8.1**
- **Vendor:** ANDRITZ
- **Equipment:** ANDRITZ HIPASE-250 and 250 SCALA
- **Vulnerabilities:** Storing Passwords in a Recoverable Format, Missing Authentication for Critical Function, Use of Hard-coded Credentials

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-65309	High	ANDRITZ HIPASE-250 (formerly 250 SCALA) in affected versions stores and transmits user passwords using a reversible format instead of a one-way password hash. This allows an attacker able to read the credential store or capture network traffic to recover all stored passwords.
CVE-2026-65310	High	ANDRITZ HIPASE-250 (formerly 250 SCALA), in the default configuration of affected versions, exposes its data and configuration endpoint without any authentication and permissive CORS on every response. An unauthenticated attacker with network access can read live process values and server configuration.
CVE-2026-65311	Medium	The HTTP server component of ANDRITZ HIPASE-250 (formerly 250 SCALA) in affected versions exposes an undocumented endpoint that changes the server's logging level and target without requiring authentication. A remote, unauthenticated

		attacker with network access to the service may suppress audit logging, potentially concealing other activity on the system.
CVE-2026-65313	High	A provisioning script used when installing HIPASE-250 (formerly 250 SCALA) engineering workstations sets a fixed, hard-coded x11vnc password. Because the same credential is applied to every workstation provisioned this way, an attacker with adjacent-network access who knows the password can gain VNC access to affected workstations.

Remediation:

- ANDRITZ has addressed these issues in version V8.00.00 (released 2024-12) and in version V8.15.00 (released 2026-07) and encourages users to keep their systems updated to the latest version (currently HIPASE-250 Version V8.15.00).

Hitachi Energy APM Edge Product

Summary

Hitachi Energy is aware of Dirty Frag vulnerabilities that affect APM Edge product versions listed in this document. Successful exploitation of these vulnerabilities could result in impact on confidentiality, integrity and availability of the product.

The following versions of Hitachi Energy APM Edge Product are affected:

- **APM Edge vers:APM_Edge/<=6.10 (CVE-2026-43284, CVE-2026-43500)**

- **CVSS v3 8.8**
- **Vendor:** Hitachi Energy
- **Equipment:** Hitachi Energy APM Edge Product
- **Vulnerabilities:** Write-what-where Condition, Out-of-bounds Write

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-43284	High	Write-what-where Condition A vulnerability exists in the IPsec ESP subsystem (esp4, esp6) of the Linux kernel used in APM Edge that allows a local unprivileged user to escalate privileges to root. The flaw exists in how the kernel handles memory pages when processing ESP encrypted network packets. An attacker can craft a packet that causes the kernel to decrypt data directly into memory pages it does not own, including the cached copies of privileged operating system binaries. When one of those binaries is executed, the attacker's injected code runs with root privileges. In APM Edge, the vulnerable kernel modules (esp4, esp6) can be loaded by any local user and exploited.
CVE-2026-43500	High	Out-of-bounds Write A vulnerability exists in the RxRPC protocol implementation of Linux kernel used in APM Edge that allows a local unprivileged user to escalate privileges to root. RxRPC incorrectly processes incoming network packets that carry externally owned memory fragments. During packet processing, the kernel writes decrypted data directly into memory pages it does not own, including cached copies of privileged operating system binaries. Upon execution of a corrupted binary, the attacker's injected code runs with root

		privileges. In APM Edge, the vulnerable kernel module (rxrpc) can be loaded by any local user and exploited.

Remediation:

- Disable the esp4 and esp6 modules
- Disable the rxrpc module

Johnson Controls Inc. Airwall

Summary

Successful exploitation of these vulnerabilities could allow an attacker to decrypt sensitive data, bypass authentication controls, gaining unauthorized access to read arbitrary files on the system, or gain unauthorized access to protected system resources.

The following versions of Johnson Controls Inc. Airwall are affected:

- **Airwall <=4.0.4 (CVE-2026-64887, CVE-2026-34492)**

- **CVSS v3 6.8**
- **Vendor:** Johnson Controls Inc.
- **Equipment:** Johnson Controls Inc. Airwall
- **Vulnerabilities:** Use of Hard-coded Cryptographic Key, External Control of File Name or Path

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-64887	High	A hardcoded password or cryptographic key was identified in the Airwall application. A hardcoded credential leads to a significant authentication failure that can be difficult for system or application administrators to detect. Once discovered, it is difficult to remediate without manually modifying or patching the software. The hardcoded key is identical across all installations of the product and across all customer organizations, meaning a single disclosure of the key - common on the internet - grants any knowledgeable attacker access to all affected deployments. An attacker with access to application code or binary files can use the hardcoded key to decrypt sensitive application data stored in configuration and database files, enabling further data disclosure or compromise of application infrastructure.
CVE-2026-34492	High	An arbitrary file read vulnerability was identified in the Airwall application. This issue occurs when user-supplied input is directly incorporated into filesystem access functions without adequate validation or sanitization. As a result, an attacker can request and obtain the contents of arbitrary files on the server, including sensitive configuration files, source code, credential stores, and private keys, provided the application process has permission to read them. The vulnerability is commonly exploited through path traversal sequences (e.g., ../) or absolute file paths (e.g., /etc/passwd). Encoding variations of traversal sequences (e.g., %2e%2e%2f) can also bypass basic filters.

Remediation:

To help reduce risk of exploitation, Johnson Controls recommends the following defensive measures:

- Apply v4.1.0 or later patches for all Airwalls.
- Store all cryptographic keys in a secure key management system (KMS) or hardware security module (HSM) rather than embedding them in source code or configuration files. (CVE-2026-64887)
- Implement a regular key rotation policy to limit the exposure window if a key is compromised. (CVE-2026-64887)
- Use unique cryptographic keys per device, installation, or deployment instance to prevent a single compromised key from affecting all installations. (CVE-2026-64887)
- Remove any hard-coded keys from source code repositories and binaries, replacing them with references to secure external key stores. (CVE-2026-64887)Apply the principle of least privilege to key access, ensuring only authorized processes and personnel can retrieve cryptographic material. (CVE-2026-64887)
- Use static analysis and secrets-scanning tools in CI/CD pipelines to detect and prevent hard-coded keys from being committed to source control. (CVE-2026-64887)
- Encrypt keys at rest and in transit and ensure key-wrapping mechanisms are in place for any keys stored on disk. (CVE-2026-64887)
- Audit and monitor access to cryptographic keys, logging all retrieval and usage events for anomaly detection. (CVE-2026-64887)
- Validate and sanitize all user-supplied input before using it in file system operations (CVE-2026-34492)
- Implement strict allowlists for permitted file paths, file names, and directories (CVE-2026-34492)
- Use canonicalization to resolve path traversal sequences before validation (CVE-2026-34492)
- Apply the principle of least privilege to the application file system access permissions (CVE-2026-34492)
- Deploy sandboxing or chroot jails to restrict the application's file system scope (CVE-2026-34492)
- Avoid passing user-controlled data directly to file system APIs (CVE-2026-34492)
- Refer to and follow all steps in the product hardening guide or the JCI universal hardening guide found here https://www.johnsoncontrols.com/trust-center/cybersecurity/resources (CVE-2026-64887, CVE-2026-34492)
- For more detailed mitigation instructions, please see Johnson Controls Product Security Advisory JCI-PSA-2026-25. (CVE-2026-64887, CVE-2026-34492)

Haiwell IoT Cloud HMI Gateway

Summary

Successful exploitation of this vulnerability may allow an attacker to inject and execute arbitrary OS commands with root privileges.

The following versions of Haiwell IoT Cloud HMI Gateway are affected:

- **Haiwell IoT Cloud HMI Gateway 3.40.1.12 (CVE-2026-19188)**

- **CVSS v3 10**
- **Vendor:** Haiwell

- **Equipment:** Haiwell IoT Cloud HMI Gateway
- **Vulnerabilities:** Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-19188	Critical	A critical OS command injection vulnerability has been identified in the Haiwell IoT Cloud HMI Gateway product. The vulnerability exists in the Net Check feature accessible via the /setting endpoint. The cmdPing Socket.io event fails to properly sanitize user-supplied input before passing it to the underlying operating system, allowing an attacker to inject and execute arbitrary OS commands with root privileges

Remediation:

- Haiwell has addressed the issue in patch version number Scada-v3.50.1.19, which is available for download on their website.

AVEVA Enterprise SCADA

Summary

Successful exploitation of this vulnerability could allow an attacker to tamper with serialized data, potentially resulting in code execution during deserialization.

The following versions of AVEVA Enterprise SCADA are affected:

- **Enterprise SCADA 2025 (CVE-2025-7639)**
- **Enterprise SCADA >=2024|<=2024_SP1_P01 (CVE-2025-7639)**
- **Enterprise SCADA >=2023|<=2023_SP1 (CVE-2025-7639)**
- **Enterprise SCADA >=2022|<=2022_SP2_P2 (CVE-2025-7639)**
- **Enterprise SCADA <=2021_SP2_P5 (CVE-2025-7639)**
- **Enterprise SCADA HMI 2024|2024|R2 (CVE-2025-7639)**
- **Enterprise SCADA HMI <=2023_P1 (CVE-2025-7639)**

- **CVSS v3 7.1**
- **Vendor:** AVEVA
- **Equipment:** AVEVA Enterprise SCADA
- **Vulnerabilities:** Deserialization of Untrusted Data

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2025-7639	High	The vulnerability, if exploited, could allow an authenticated miscreant with "DNA Authority - Operator" privilege to tamper with serialized data, potentially resulting in code execution during deserialization under the privilege of Enterprise SCADA security group "DNA Apps".

Remediation:

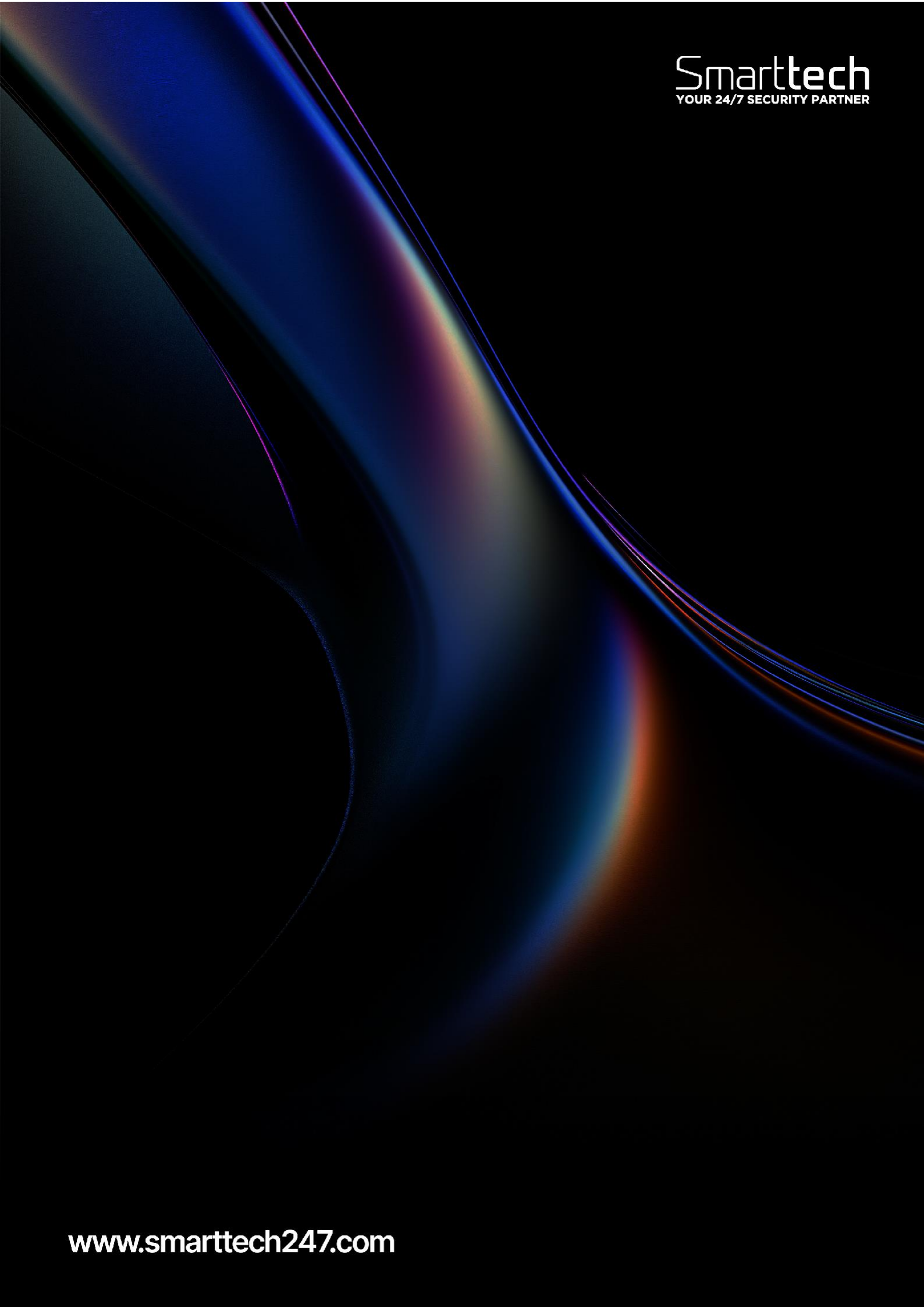
- AVEVA recommends that customers using affected product versions should perform the following to mitigate the risk of exploit:
  1. Evaluate the impact of these vulnerabilities based on your operational environment, architecture, and product implementation.
  2. Plan an upgrade of Servers and Clients to one of the available fixed versions listed in this document.
  3. Configure Servers and Clients as described in this document.
- Contact your AVEVA Technical Support representative, Customer Success Manager, Account Manager, or Solution Integrator to obtain the security update best applicable to the product version currently deployed in your environment: Servers: AVEVA Enterprise SCADA v2025 P1 or higher, AVEVA Enterprise SCADA v2024 SP1 P2, AVEVA Enterprise SCADA v2023 SP1 P1, AVEVA Enterprise SCADA v2022 SP2 P3, AVEVA Enterprise SCADA v2021 SP2 P6, AVEVA Pipeline Operations for Gas/Liquids v2025 P1 or higher, AVEVA Pipeline Operations for Gas/Liquids v2024 SP1 P2, AVEVA Pipeline Operations for Gas/Liquids v2023 SP1 P1, AVEVA Pipeline Operations for Gas/Liquids v2022 SP2 P3, AVEVA Pipeline Operations for Gas/Liquids v2021 SP2 P6 Clients: AVEVA Enterprise SCADA HMI v2024 R2 HF7 or higher, AVEVA Enterprise SCADA HMI v2024 P1, AVEVA Enterprise SCADA HMI v2023 P2 HF1, AVEVA Pipeline Integrity Monitor (delivered on Pipeline Simulation media) v2025 SP1 P2 or higher, AVEVA Pipeline Training Simulator (delivered on Pipeline Simulation media) v2025 SP1 P2 or higher, Measurement Advisor 2025 P1 or higher, Measurement Advisor 2021 SP1 HF16.
- To fully mitigate the risk of exploit, the following configuration changes must be implemented after all server and client nodes have been upgraded to compatible versions that support the fix:Server Components: Change "BinarySerializer" -> "Mode" setting from 'Binary Formatter' to 'Json'. Change "BinarySerializer" -> "AcceptBinaryFormattedData" setting from 'true' to 'false'. Re-cache the XOS Event Handlers assembly.
- Client Components: Configure clients/products that interface with Enterprise SCADA to only use JSON serialization.
- HMI: Migrate HMI displays.
- For step-by-step instructions on where and how to apply these configuration settings, how to migrate HMI displays, compatible server-client versions list, and additional details please refer to KB117814 "AVEVA Midstream Product Bulletin - Removal of Binary Formatter".
- AVEVA recommends the following general defensive measures:
  1. Audit devices, network topology, and perimeter defences to ensure all applicable security best practices from AVEVA's Enterprise SCADA Reference System Architecture are adhered to.
  2. Audit assigned permissions to ensure that only trusted users are given "DNA Authority - Operator" rights.
  3. Disallow BLT Test clients in production environments.
- For more information on this vulnerability, including security updates, users should see the security bulletin AVEVA-2026-005.

References

https://www.cisa.gov/news-events/ics-advisories/icsa-26-225-14
https://www.cisa.gov/news-events/ics-medical-advisories/icsma-26-225-01
https://www.cisa.gov/news-events/ics-advisories/icsa-26-225-13
https://www.cisa.gov/news-events/ics-advisories/icsa-26-225-12
https://www.cisa.gov/news-events/ics-advisories/icsa-26-225-11
https://www.cisa.gov/news-events/ics-advisories/icsa-26-225-10
https://www.cisa.gov/news-events/ics-advisories/icsa-26-225-09
https://www.cisa.gov/news-events/ics-advisories/icsa-26-225-08
https://www.cisa.gov/news-events/ics-advisories/icsa-26-225-07
https://www.cisa.gov/news-events/ics-advisories/icsa-26-225-05
https://www.cisa.gov/news-events/ics-advisories/icsa-26-225-04
https://www.cisa.gov/news-events/ics-advisories/icsa-26-225-03
https://www.cisa.gov/news-events/ics-advisories/icsa-26-225-02
https://www.cisa.gov/news-events/ics-advisories/icsa-26-225-01
https://github.com/V4bel/dirtyfrag

CVEs

CVE-2026-34491
CVE-2026-18164
CVE-2026-57262
CVE-2026-57263
CVE-2026-50058
CVE-2026-50059
CVE-2026-50060
CVE-2026-50061
CVE-2026-50062
CVE-2026-50063
CVE-2026-50064
CVE-2026-59700
CVE-2026-59701
CVE-2026-64629
CVE-2026-3014
CVE-2026-59693
CVE-2026-69108
CVE-2026-69109
CVE-2026-65309
CVE-2026-65310
CVE-2026-65311
CVE-2026-65313
CVE-2026-43284
CVE-2026-43500
CVE-2026-64887
CVE-2026-34492
CVE-2026-19188
CVE-2025-7639


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com