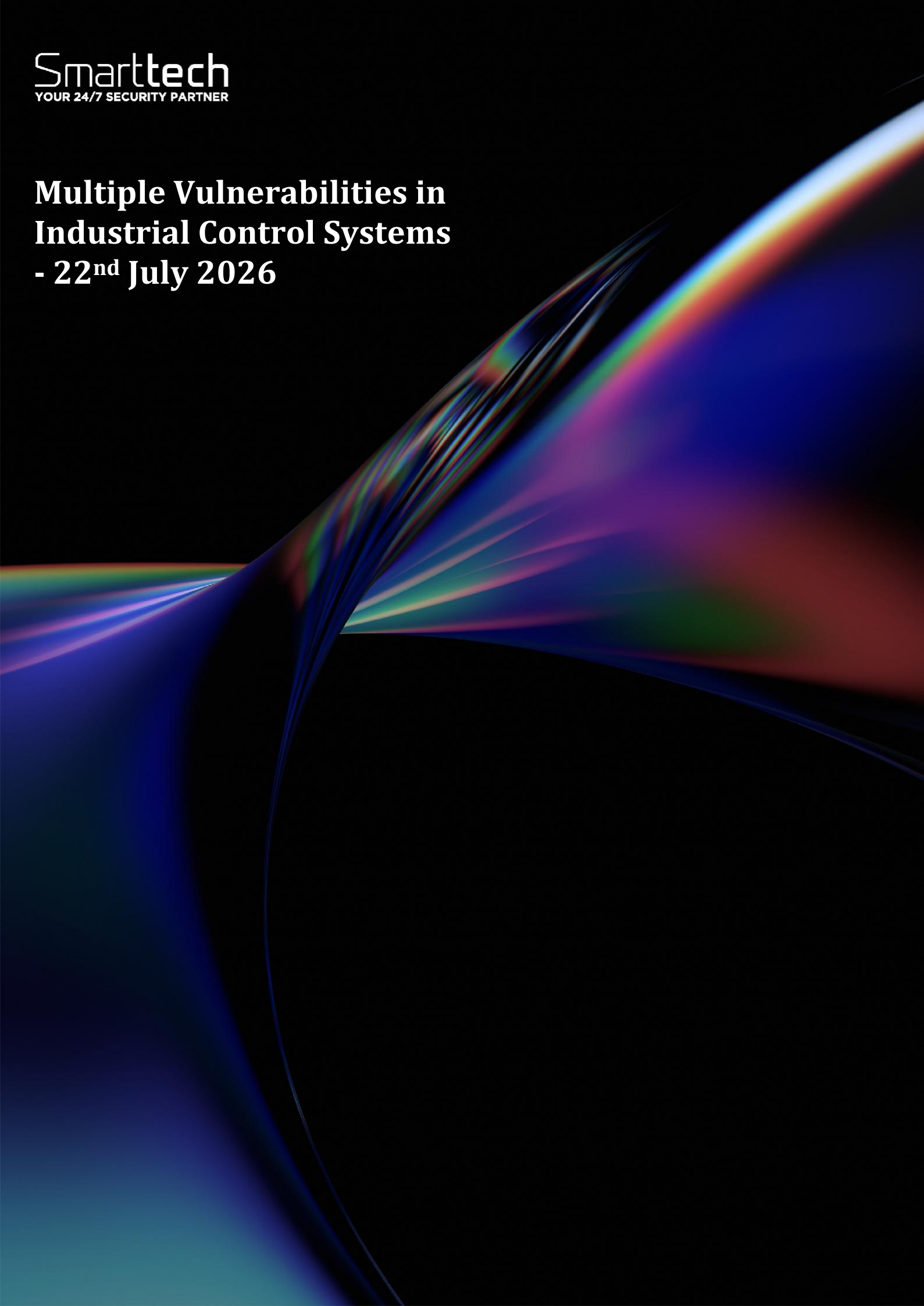
Smarttech
YOUR 24/7 SECURITY PARTNER

# Multiple Vulnerabilities in Industrial Control Systems - 22nd July 2026



| | |
|---|---|
| **Document ID** | SMA-Threat Report |
| **Document status** | ISSUED |
| **Issue Number** | 121 |
| **Authors** | Dorin Constantin Banu < constantin.banu@smarttech247.com > |
| **Verified by** | Alin Curcan < alin.curcan@smarttech247.com > |
| **Last modified** | 2026-07-22 |
| **Issue Date** | 2026-07-21 |

**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: **Rockwell Automation Studio 5000 Logix Designer**, **Rockwell Automation 1734 POINT I/O, Rockwell Automation 1718-AENTR/1719-AENTR, Rockwell Automation FactoryTalk Services Platform, Siemens CADRA, Siemens IAM Client, Siemens SIDIS Secured SmartPlug, Siemens Opcenter X, Siemens RUGGEDCOM APE1808 with Palo Alto Networks Virtual NGFW**, and **Tycon Systems TPDIN-Monitor-WEB2**. Successful exploitation of these vulnerabilities could enable authentication bypass and unauthorized access, privilege escalation, arbitrary code execution, information disclosure, cross-site scripting, and denial-of-service conditions.

## Rockwell Automation Studio 5000 Logix Designer

### Summary

Successful exploitation of these vulnerabilities could allow for a local attacker to execute arbitrary files, alter configurations, or execute arbitrary code.

The following versions of Rockwell Automation Studio 5000 Logix Designer are affected:

- **Studio 5000 Logix Designer V36.00 (CVE-2026-9108)**
- **Studio 5000 Logix Designer V35.00 (CVE-2026-9108, CVE-2026-9127, CVE-2026-9128)**
- **Studio 5000 Logix Designer V35.01 (CVE-2026-9108)**
- **Studio 5000 Logix Designer >=V34.00|<=V34.03 (CVE-2026-9108)**
- **Studio 5000 Logix Designer >=V33.00|<=V33.03 (CVE-2026-9108)**
- **Studio 5000 Logix Designer >=V32.00|<=V32.04 (CVE-2026-9108, CVE-2026-9127, CVE-2026-9128)**
- **Studio 5000 Logix Designer V34.00 (CVE-2026-9127)**
- **Studio 5000 Logix Designer V34.01 (CVE-2026-9127)**
- **Studio 5000 Logix Designer V33.00 (CVE-2026-9127)**
- **Studio 5000 Logix Designer V33.02 (CVE-2026-9127)**
- **Studio 5000 Logix Designer >=V34.00|<=V34.02 (CVE-2026-9128)**
- **Studio 5000 Logix Designer >=V33.00|<=V33.02 (CVE-2026-9128)**

- **CVSS v3 7.5**
- **Vendor:** Rockwell Automation

- **Equipment:** Rockwell Automation Studio 5000 Logix Designer
- **Vulnerabilities:** Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Incorrect Authorization, Unquoted Search Path or Element

**Vulnerabilities**

| CVE ID | Base Severity | Description |
|---|---|---|
| **CVE-2026-9108** | Medium | A path traversal security issue exists within Studio 5000 Logix Designer due to improper limitation of file paths within ACD project files. The software does not sanitize or validate file names embedded in the ACD file structure during the project opening procedure, allowing path traversal sequences to escape the intended extraction directory. If exploited, an attacker could craft a malicious ACD project file that results in arbitrary files being written to attacker-controlled locations on the file system, potentially leading to code execution. |
| **CVE-2026-9127** | High | A remote code execution security issue exists within Studio 5000 Logix Designer due to incorrect authorization on a configuration file. This can allow any authenticated user to modify the paths of external tools configured within the application. If exploited, an attacker could alter the configuration to point to a malicious executable, resulting in arbitrary code execution when any user interacts with the external tools functionality. |
| **CVE-2026-9128** | High | A code execution security issue exists within Studio 5000 Logix Designer due to an unquoted search path in the External Tools configuration. The executable paths specified in the external tools configuration file are not properly quoted, and because these paths contain spaces, the operating system may resolve them to unintended executables placed earlier in the search order. If exploited, an attacker could plant a malicious executable in a location within the search path, resulting in arbitrary code execution with the same permissions of the user running the application. |

**Remediation:**

- Rockwell Automation recommends users to upgrade to the following: Studio 5000 Logix Designer: V37.00, 36.01, 35.02, 34.04, 33.04, 32.05 (CVE-2026-9108).
- Studio 5000 Logix Designer: V36.00, 35.01, 34.02, 33.02, 32.05 (CVE-2026-9127).
- Studio 5000 Logix Designer: V36.00, 35.01, 34.03, 33.03, 32.05 (CVE-2026-9128).
- Customers using the affected software, who are not able to upgrade to one of the corrected versions, should use Rockwell Automation's security best practices

## Rockwell Automation 1734 POINT I/O

**Summary**

Successful exploitation of this vulnerability could allow for an attacker to cause a denial-of-service condition on the product.

The following versions of Rockwell Automation 1734 POINT I/O are affected:

- **1734 POINT I/O 3.023**

- **CVSS v3 7.5**
- **Vendor:** Rockwell Automation
- **Equipment:** Rockwell Automation 1734 POINT I/O
- **Vulnerabilities:** Allocation of Resources Without Limits or Throttling

**Vulnerabilities**

| CVE ID | Base Severity | Description |
|---|---|---|
| **CVE-2026-10573** | High | A denial-of-service security issue exists in 1734 POINT I/O module. The security issue stems from improper handling of crafted CIP messages, which can cause the module to enter a faulted state. A restart is required to recover. |

**Remediation:**

- Rockwell Automation recommends users are to migrate to 5034-OB8.
- Customers using the affected software, who are not able to upgrade to one of the corrected versions, should use Rockwell Automation's security best practices.

## Rockwell Automation 1718-AENTR/1719-AENTR

**Summary**

Successful exploitation of this vulnerability could allow for an attacker to cause a denial-of-service condition on the product.

The following versions of Rockwell Automation 1718-AENTR/1719-AENTR are affected:

- **1718/ 1719 Ex I/O 3.011**

- **CVSS v3 7.5**
- **Vendor:** Rockwell Automation
- **Equipment:** Rockwell Automation 1718-AENTR/1719-AENTR
- **Vulnerabilities:** Allocation of Resources Without Limits or Throttling

**Vulnerabilities**

| CVE ID | Base Severity | Description |
|---|---|---|
| **CVE-2026-9140** | High | A denial-of-service security issue exists in the 1719-AENTR. The security issue stems from improper handling of a UDP unicast network storm, which causes the device to become overloaded and lose communication. A power cycle is required to recover. |

**Remediation:**

- Rockwell Automation recommends users to upgrade to 1718/ 1719 Ex I/O version 3.012 or later.
- Customers using the affected software, who are not able to upgrade to one of the corrected versions, should use Rockwell Automation's security best practices.

## Rockwell Automation FactoryTalk Services Platform

### Summary

Successful exploitation of this vulnerability could allow an attacker to impersonate an authorized user on the FTSP server, resulting in unauthorized access to system configurations.

The following versions of Rockwell Automation FactoryTalk Services Platform are affected:

- **FactoryTalk Directory (FTSP) 6.60**

- **CVSS v3 7.8**
- **Vendor:** Rockwell Automation
- **Equipment:** Rockwell Automation FactoryTalk Services Platform
- **Vulnerabilities:** Weak Authentication

### Vulnerabilities

| CVE ID | Base Severity | Description |
|---|---|---|
| **CVE-2026-10714** | High | A security issue exists within FactoryTalk Services Platform (FTSP), allowing an attacker to bypass JWT signature validation during Okta Web Authentication. The vulnerability stems from the application not verifying that the JWT algorithm is configured for RSA, enabling an attacker to set the algorithm to "none" and craft forged tokens. This could allow an authenticated low-privilege user to impersonate any authorized user on the FTSP server, resulting in unauthorized access to system configuration and the ability to grant permissions to other systems protected by FTSP. |

### Remediation:

- Users using FactoryTalk Services Platform v6.60 should apply either the individual patch (RAID 1158263) or the February 2026 Patch Roll-up, or later update.
- Users using the affected software, who are not able to upgrade to one of the corrected versions, should use Rockwell's security best practices.

## Siemens CADRA

### Summary

CADRA is affected by multiple zlib and Foxit vulnerabilities. Siemens has released a new version for CADRA and recommends to update to the latest version. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.

The following versions of Siemens CADRA are affected:

- **CADRA vers:intdot/<2511, vers:all/***

- **CVSS v3 9.8**
- **Vendor:** Siemens
- **Equipment:** Siemens CADRA

- **Vulnerabilities:** Improper Input Validation, Incorrect Bitwise Shift of Integer, Out-of-bounds Write, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Integer Overflow or Wraparound, Access of Resource Using Incompatible Type ('Type Confusion')

**Vulnerabilities**

| CVE ID | Base Severity | Description |
|---|---|---|
| **CVE-2005-2096** | High | zlib 1.2 and later versions allows remote attackers to cause a denial of service (crash) via a crafted compressed stream with an incomplete code description of a length greater than 1, which leads to a buffer overflow, as demonstrated using a crafted PNG file. |
| **CVE-2016-9840** | High | inftrees.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic. |
| **CVE-2016-9841** | Critical | inffast.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic. |
| **CVE-2016-9842** | High | The inflateMark function in inflate.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact via vectors involving left shifts of negative integers. |
| **CVE-2017-14919** | High | Node.js before 4.8.5, 6.x before 6.11.5, and 8.x before 8.8.0 allows remote attackers to cause a denial of service (uncaught exception and crash) by leveraging a change in the zlib module 1.2.9 making 8 an invalid value for the windowBits parameter. |
| **CVE-2018-25032** | High | zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches. |
| **CVE-2022-37434** | Critical | zlib through 1.2.12 has a heap-based buffer over-read or buffer overflow in inflate in inflate.c via a large gzip header extra field. NOTE: only applications that call inflateGetHeader are affected. Some common applications bundle the affected zlib source code but may be unable to call inflateGetHeader (e.g., see the nodejs/node reference). |
| **CVE-2023-45853** | Critical | MiniZip in zlib through 1.3 has an integer overflow and resultant heap-based buffer overflow in zipOpenNewFileInZip4_64 via a long filename, comment, or extra field. NOTE: MiniZip is not a supported part of the zlib product. NOTE: pyminizip through 0.2.6 is also vulnerable because it bundles an affected zlib version, and exposes the applicable MiniZip code through its compress API. |
| **CVE-2025-10585** | High | Type confusion in V8 in Google Chrome prior to 140.0.7339.185 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) |
| **CVE-2025-13223** | High | Type Confusion in V8 in Google Chrome prior to 142.0.7444.175 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. |
| **CVE-2026-22184** | - | zlib versions up to and including 1.3.1.2 include a global buffer overflow in the untgz utility located under contrib/untgz. The vulnerability is limited to the standalone demonstration utility and does not affect the core zlib compression library. The flaw occurs when a user executes the untgz command with an excessively long archive name supplied via the command line, leading to an out-of-bounds write in a fixed-size global buffer. |

**Remediation:**

- Update to V2511 or later version
- Block access to untrusted or external web content from sensitive systems
- Currently no fix is available for CVE-2026-22184.

## Siemens IAM Client

**Summary**

Multiple Siemens products are affected by unquoted search path vulnerability in IAM Client. This could allow an authenticated local attacker to perform privilege escalation. Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends countermeasures for products where fixes are not, or not yet available.

The following versions of Siemens IAM Client are affected:

- **COMOS V10.4.5 vers:intdot/<10.4.5.0.2**
- **COMOS V10.6 vers:intdot/<10.6.1**
- **Designcenter NX vers:intdot/<2512.7000**
- **Simcenter 3D vers:intdot/<2512.7000**
- **Simcenter Femap V2506 vers:intdot/<2506.0003**
- **Simcenter Femap V2512 vers:intdot/<2512.0002**
- **Simcenter Nastran vers:intdot/<2606**
- **Simcenter STAR-CCM+ vers:intdot/<2606**
- **Solid Edge SE2025 vers:intdot/<225.0.13.3**
- **Solid Edge SE2026 vers:intdot/<226.0.04.003**
- **Teamcenter Visualization V2412 vers:intdot/<2412.0012**
- **Teamcenter Visualization V2506 vers:intdot/<2506.0009**
- **Teamcenter Visualization V2512 vers:intdot/<2512.2605**
- **Tecnomatix Plant Simulation V2404 vers:intdot/<2404.0022**
- **Tecnomatix Plant Simulation V2504 vers:intdot/<2504.0010**
- **Tecnomatix Process Simulate vers:intdot/<2606**

- **CVSS v3 6.7**
- **Vendor:** Siemens
- **Equipment:** Siemens IAM Client
- **Vulnerabilities:** Untrusted Search Path

**Vulnerabilities**

| CVE ID | Base Severity | Description |
|---|---|---|
| **CVE-2025-40945** | Medium | Untrusted search path in IAM Client SDK may allow an authenticated user to potentially enable escalation of privilege via local access. |

**Remediation:**

- Update to V10.6.1 or later version
- Update to V225.0 Update 13 or later version
- Update to V226.0 Update 04 or later version

- Update to V2404.0022 or later version
- Update to V2412.0012 or later version
- Update to V2504.0010 or later version
- Update to V2506.0003 or later version
- Update to V2506.0009 or later version
- Update to V2512.0002 or later version
- Update to V2512.2605 or later version
- Update to V2512.7000 or later version
- Update to V2512.7000 or later version
- Update to V2606 or later version
- Update to V10.4.5.0.2 or later version. Contact customer support to receive patch and update information

## Siemens SIDIS Secured SmartPlug

### Summary

SIDIS Secured SmartPlug before V7.26.0310 is affected by multiple vulnerabilities in the components OpenSSL, OpenSSH, and several other packages as described below. Siemens has released a new version of SIDIS Secured SmartPlug and recommends to update to the latest version.

The following versions of Siemens SIDIS Secured SmartPlug are affected:

- **SIDIS Secured SmartPlug vers:intdot/<7.26.0310**

- **CVSS v3 9.8**
- **Vendor:** Siemens
- **Equipment:** Siemens SIDIS Secured SmartPlug
- **Vulnerabilities:** Improper Enforcement of Message Integrity During Transmission in a Communication Channel, Reusing a Nonce, Key Pair in Encryption, Out-of-bounds Write, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Integer Overflow or Wraparound, Out-of-bounds Read, Covert Timing Channel, Detection of Error Condition Without Action, Incorrect Authorization

### Vulnerabilities

| CVE ID | Base Severity | Description |
|---|---|---|
| **CVE-2022-23303** | Critical | The implementations of SAE in hostapd before 2.10 and wpa_supplicant before 2.10 are vulnerable to side channel attacks as a result of cache access patterns. NOTE: this issue exists because of an incomplete fix for CVE-2019-9494. |
| **CVE-2022-23304** | High | The implementations of EAP-pwd in hostapd before 2.10 and wpa_supplicant before 2.10 are vulnerable to side-channel attacks as a result of cache access patterns. NOTE: this issue exists because of an incomplete fix for CVE-2019-9495. |
| **CVE-2022-37660** | Medium | In hostapd 2.10 and earlier, the PKEX code remains active even after a successful PKEX association. An attacker that successfully bootstrapped public keys with another entity using PKEX in the past, will be able to subvert a future bootstrapping by passively observing public keys, re-using the encrypting element Qi and subtracting it from the captured message M (X = M - Qi). This will result in the public ephemeral key X; the only element required |

| | | |
|---|---|---|
| | | to subvert the PKEX association. |
| **CVE-2022-48174** | High | There is a stack overflow vulnerability in ash.c:6030 in busybox before 1.35. In the environment of Internet of Vehicles, this vulnerability can be executed from command to arbitrary code execution. |
| **CVE-2025-5222** | High | A stack buffer overflow was found in Internationl components for unicode (ICU ). While running the genrb binary, the 'subtag' struct overflowed at the SRBRoot::addTag function. This issue may lead to memory corruption and local arbitrary code execution. |
| **CVE-2025-5914** | High | A vulnerability has been identified in the libarchive library, specifically within the archive_read_format_rar_seek_data() function. This flaw involves an integer overflow that can ultimately lead to a double-free condition. Exploiting a double-free vulnerability can result in memory corruption, enabling an attacker to execute arbitrary code or cause a denial-of-service condition. |
| **CVE-2025-9230** | High | An application trying to decrypt CMS messages encrypted using password based encryption can trigger an out-of-bounds read and write. Impact summary: This out-of-bounds read may trigger a crash which leads to Denial of Service for an application. The out-of-bounds write can cause a memory corruption which can have various consequences including a Denial of Service or Execution of attacker-supplied code. Although the consequences of a successful exploit of this vulnerability could be severe, the probability that the attacker would be able to perform it is low. Besides, password based (PWRI) encryption support in CMS messages is very rarely used. For that reason the issue was assessed as Moderate severity according to our Security Policy. The FIPS modules in 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this issue, as the CMS implementation is outside the OpenSSL FIPS module boundary. |
| **CVE-2025-9231** | Medium | A timing side-channel which could potentially allow remote recovery of the private key exists in the SM2 algorithm implementation on 64 bit ARM platforms. Impact summary: A timing side-channel in SM2 signature computations on 64 bit ARM platforms could allow recovering the private key by an attacker.. While remote key recovery over a network was not attempted by the reporter, timing measurements revealed a timing signal which may allow such an attack. OpenSSL does not directly support certificates with SM2 keys in TLS, and so this CVE is not relevant in most TLS contexts. However, given that it is possible to add support for such certificates via a custom provider, coupled with the fact that in such a custom provider context the private key may be recoverable via remote timing measurements, we consider this to be a Moderate severity issue. The FIPS modules in 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this issue, as SM2 is not an approved algorithm. |
| **CVE-2025-9232** | Medium | An application using the OpenSSL HTTP client API functions may trigger an out-of-bounds read if the 'no_proxy' environment variable is set and the host portion of the authority component of the HTTP URL is an IPv6 address. Impact summary: An out-of-bounds read can trigger a crash which leads to Denial of Service for an application. The OpenSSL HTTP client API functions can be used directly by applications but they are also used by the OCSP client functions and CMP (Certificate Management Protocol) client implementation in OpenSSL. However the URLs |

| | | |
|---|---|---|
| | | used by these implementations are unlikely to be controlled by an attacker. In this vulnerable code the out of bounds read can only trigger a crash. Furthermore the vulnerability requires an attacker-controlled URL to be passed from an application to the OpenSSL function and the user has to have a 'no_proxy' environment variable set. For the aforementioned reasons the issue was assessed as Low severity. The vulnerable code was introduced in the following patch releases: 3.0.16, 3.1.8, 3.2.4, 3.3.3, 3.4.0 and 3.5.0. The FIPS modules in 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this issue, as the HTTP client implementation is outside the OpenSSL FIPS module boundary. |
| **CVE-2025-26465** | Medium | A vulnerability was found in OpenSSH when the VerifyHostKeyDNS option is enabled. A machine-in-the-middle attack can be performed by a malicious machine impersonating a legit server. This issue occurs due to how OpenSSH mishandles error codes in specific conditions when verifying the host key. For an attack to be considered successful, the attacker needs to manage to exhaust the client's memory resource first, turning the attack complexity high. |
| **CVE-2025-32462** | Low | Sudo before 1.9.17p1, when used with a sudoers file that specifies a host that is neither the current host nor ALL, allows listed users to execute commands on unintended machines. |
| **CVE-2026-5121** | High | A flaw was found in libarchive. On 32-bit systems, an integer overflow vulnerability exists in the zisofs block pointer allocation logic. A remote attacker can exploit this by providing a specially crafted ISO9660 image, which can lead to a heap buffer overflow. This could potentially allow for arbitrary code execution on the affected system. |

**Remediation:**

- Update to V7.26.0310 or later version.

## Siemens Opcenter X

**Summary**

Opcenter X before V2604 contains an authentication bypass vulnerability that could allow an attacker to gain full unauthorized access to the application. Siemens has released a new version for Opcenter X and recommends to update to the latest version.

The following versions of Siemens Opcenter X are affected:

- **Opcenter X vers:intdot/<2604**

- **CVSS v3 10**
- **Vendor:** Siemens
- **Equipment:** Siemens Opcenter X
- **Vulnerabilities:** Improper Verification of Cryptographic Signature

**Vulnerabilities**

| CVE ID | Base Severity | Description |
|---|---|---|
| **CVE-2026-56451** | Critical | Affected applications do not properly validate the algorithm specified in the JSON Web Token (JWT) header. This could allow |

| | | |
|---|---|---|
| | | an unauthenticated remote attacker to forge arbitrary JWT, bypass authentication mechanisms and impersonate any user including administrative accounts, potentially gaining full unauthorized access to the application. |

**Remediation:**

- Update to V2604 or later version.

## Siemens RUGGEDCOM APE1808 with Palo Alto Networks Virtual NGFW

**Summary**

Palo Alto Networks has published information on vulnerabilities in PAN-OS. This advisory lists the related Siemens Industrial products affected by these vulnerabilities. Customers are advised to consult and implement the workarounds provided in Palo Alto Networks' upstream security notifications.

The following versions of Siemens RUGGEDCOM APE1808 with Palo Alto Networks Virtual NGFW are affected:

- **RUGGEDCOM APE1808 vers:all/***

- **CVSS v3 7.2**
- **Vendor:** Siemens
- **Equipment:** Siemens RUGGEDCOM APE1808 with Palo Alto Networks Virtual NGFW
- **Vulnerabilities:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Missing Authorization, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

**Vulnerabilities**

| CVE ID | Base Severity | Description |
|---|---|---|
| **CVE-2026-0266** | Low | A cross-site scripting (XSS) vulnerability in Palo Alto Networks PAN-OS® software enables a malicious authenticated administrator to store a JavaScript payload using the web interface. This issue is applicable to PAN-OS software on PA-Series and VM-Series firewalls and on Panorama (virtual and M-Series). Cloud NGFW and Prisma® Access are not affected by this vulnerability. |
| **CVE-2026-0272** | Medium | A privilege escalation vulnerability in Palo Alto Networks PAN-OS® software allows an authenticated administrator with access to the Command Line Interface (CLI) to perform actions on the device with root privileges. The security risk posed by this issue is significantly minimized when CLI access is restricted to a limited group of administrators and by restricting access to the management interface to only trusted internal IP addresses according to our recommended best practice deployment guidelines. This issue is applicable to PAN-OS software on PA-Series and VM-Series firewalls and on Panorama (virtual and M-Series). Cloud NGFW, and Prisma® Access are not impacted by this vulnerability. |
| **CVE-2026-0273** | | A command injection vulnerability in Palo Alto Networks PAN-OS® software enables an authenticated administrator to bypass system restrictions and run arbitrary commands as a root user. |

| | | |
|---|---|---|
| | | To be able to exploit this issue, the user must have access to the PAN-OS CLI or Web UI. The security risk posed by this issue is significantly minimized when CLI access is restricted to a limited group of administrators and by restricting access to the management web interface to only trusted internal IP addresses according to our recommended best practice deployment guidelines. This issue is applicable to PAN-OS software on PA-Series and VM-Series firewalls and on Panorama (virtual and M-Series). Cloud NGFW and Prisma® Access are not affected by this vulnerability. |

**Remediation:**

- Contact customer support to receive patch and update information

## Tycon Systems TPDIN-Monitor-WEB2

**Summary**

Successful exploitation of these vulnerabilities could result in an attacker accessing sensitive credentials, disrupting connected infrastructure, or manipulating physical equipment, which could present a physical safety risk.

The following versions of Tycon Systems TPDIN-Monitor-WEB2 are affected:

- **TPDIN-Monitor-WEB2 2.3.9**

- **CVSS v3 9.8**
- **Vendor:** Tycon Systems
- **Equipment:** Tycon Systems TPDIN-Monitor-WEB2
- **Vulnerabilities:** Authentication Bypass Using an Alternate Path or Channel, Cleartext Storage of Sensitive Information

**Vulnerabilities**

| CVE ID | Base Severity | Description |
|---|---|---|
| **CVE-2026-61884** | Critical | The web management interface of the affected device does not perform server-side validation of credentials during the login process. By submitting empty values for both credential fields, an unauthenticated remote attacker can bypass the authentication check and establish a valid administrative session. This grants full access to device controls including power relay management, device reboot, remote access service configuration, and network settings, which could allow an attacker to disrupt connected infrastructure or cause physical damage to equipment. |
| **CVE-2026-55985** | Medium | The device's web management interface stores and displays system credentials in cleartext on a certain configuration page accessible to authenticated users. Any party with access to the administrative dashboard can immediately read these credentials, which may be used to compromise other systems on the local network. |

**Remediation:**

- Tycon Systems did not respond to CISA's attempts at coordination. Users of Tycon Systems TPDIN-Monitor-WEB2 are encouraged to contact Tycon Systems and keep their systems up to date.

## References

https://www.cisa.gov/news-events/ics-advisories/icsa-26-202-10
https://www.cisa.gov/news-events/ics-advisories/icsa-26-202-09
https://www.cisa.gov/news-events/ics-advisories/icsa-26-202-08
https://www.cisa.gov/news-events/ics-advisories/icsa-26-202-07
https://www.cisa.gov/news-events/ics-advisories/icsa-26-202-06
https://www.cisa.gov/news-events/ics-advisories/icsa-26-202-05
https://www.cisa.gov/news-events/ics-advisories/icsa-26-202-04
https://www.cisa.gov/news-events/ics-advisories/icsa-26-202-03
https://www.cisa.gov/news-events/ics-advisories/icsa-26-202-02
https://www.cisa.gov/news-events/ics-advisories/icsa-26-202-01

## CVEs

CVE-2026-61884
CVE-2026-55985
CVE-2026-0266
CVE-2026-0272
CVE-2026-0273
CVE-2026-56451
CVE-2022-23303
CVE-2022-23304
CVE-2022-37660
CVE-2025-32462
CVE-2025-9232
CVE-2025-9230
CVE-2025-40945
CVE-2025-10585
CVE-2017-14919
CVE-2022-37434
CVE-2026-22184
CVE-2016-9842
CVE-2023-45853
CVE-2016-9840
CVE-2018-25032
CVE-2026-10714
CVE-2026-9140
CVE-2026-10573
CVE-2026-9108
CVE-2026-9127
CVE-2026-9128

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com