Smarttech
YOUR 24/7 SECURITY PARTNER

Multiple Vulnerabilities in Industrial Control Systems - 16th September 2026

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	165
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-09-16
Issue Date	2026-09-15

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: CareCam CM2507, Siemens Teamcenter, Siemens Mendix SAML, Siemens Reyrolle 7SR5, Schneider Electric SCADAPack x70 Products, mySCADA myPRO Manager, Wärtsilä FOS-Onboard, and Digital Watchdog VMAX DVR and NVR Product Lineups. Successful exploitation of the vulnerabilities addressed in these advisories could result in unauthorized access, remote code execution, information disclosure, authentication bypass, session hijacking, credential theft, privilege escalation, unauthorized configuration changes, unauthorized software updates, and denial-of-service conditions on affected systems.

CareCam CM2507

Summary

Successful exploitation of these vulnerabilities could allow an attacker to access live video and sensitive device information, enable unauthorized services, execute arbitrary code, modify device operation, and recover stored credentials.

The following versions of CareCam CM2507 are affected:

- **HMT.CM2507 Firmware v251211.1507 (CVE-2026-88259, CVE-2026-84398, CVE-2026-84400, CVE-2026-81305, CVE-2026-85478, CVE-2026-85497, CVE-2026-81321)**

- **CVSS v3 7.5**
- **Vendor:** CareCam
- **Equipment:** CareCam CM2507
- **Vulnerabilities:** Missing Authentication for Critical Function, Empty Password in Configuration File, Inclusion of Functionality from Untrusted Control Sphere, Use of Password Hash With Insufficient Computational Effort, Cleartext Storage of Sensitive Information

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-88259	High	CareCam CM2507 IP cameras do not require authentication for access to its network video streaming service. An unauthenticated attacker

		with network access to the affected device could retrieve live camera video.
CVE-2026-84398	High	CM2507 IP cameras accept an empty password for a privileged account exposed through its ONVIF management service. An attacker with network access to the affected device could access privileged management functions and obtain device, user, media-profile, and stream configuration information.
CVE-2026-84400	Low	CareCam CM2507 IP cameras contain an insufficiently protected network maintenance mechanism that can activate a remote debugging service. An attacker on the same local network who satisfies certain device state conditions could make the service remotely accessible, increasing the risk of unauthorized administrative access.
CVE-2026-81305	Medium	CM2507 IP cameras automatically execute a predetermined script from removable media without verifying its authenticity or integrity. An attacker with physical access to the device could supply a malicious script and execute arbitrary code in the security context of the affected device.
CVE-2026-85478	Low	A CM2507 IP camera running firmware version HMT.CM2507 v251211.1507 exposes an interactive bootloader through a physical debug interface without requiring authentication. An attacker with physical access could interrupt the normal boot process and access functionality that permits inspection or modification of boot configuration, firmware data, and software loaded by the device.
CVE-2026-85497	High	CareCam CM2507 IP cameras store the device's root-account password using a fixed legacy password hash that provides insufficient resistance to offline cracking. An attacker who obtains the firmware image or password database could recover the associated credential, which may also be reusable across other devices running the same firmware.
CVE-2026-81321	High	CM2507 IP cameras store configured wireless network credentials in cleartext within the device filesystem. An attacker who obtains filesystem access through physical access, a debugging interface, or another vulnerability could recover the configured network identifier and pre-shared key.

Remediation:

- CareCam has not responded to CISA's attempts to coordinate. Users are encouraged to reach out to CareCam for more information.

Siemens Teamcenter

Summary

A reflected cross site scripting vulnerability in the authentication redirect flow (/auth/) of Teamcenter allows an unauthenticated remote attacker to inject JavaScript into an authenticated user's session by crafting a malicious URL. Successful exploitation may enable the attacker to read data or perform actions within the victim's Teamcenter session. Siemens has released new versions for the affected products and recommends to update to the latest versions.

The following versions of Siemens Teamcenter are affected:

- **Teamcenter V2412 vers:intdot/<2412.0013 (CVE-2026-58113)**
- **Teamcenter V2506 vers:intdot/<2506.0010 (CVE-2026-58113)**
- **Teamcenter V2512 vers:intdot/<2512.2607 (CVE-2026-58113)**

- **Teamcenter V2606 vers:intdot/<2606.2607 (CVE-2026-58113)**

- **CVSS v3 6.1**
- **Vendor:** Siemens
- **Equipment:** Siemens Teamcenter
- **Vulnerabilities:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-58113	Medium	Affected applications do not properly encode user-supplied input reflected into HTML attribute contexts within the authentication redirect flow (/auth/ endpoint). This could allow an unauthenticated remote attacker to inject arbitrary JavaScript into the browser of an authenticated user who loads a crafted URL, enabling the attacker to perform actions within the victim's Teamcenter session.

Remediation:

- Update to V2412.0013 or later version
- Update to V2506.0010 or later version
- Update to V2512.2607 or later version
- Update to V2606.2607 or later version

Siemens Mendix SAML

Summary

Mendix SAML module contains a vulnerability that could allow unauthenticated remote attackers to hijack an account in specific SSO configurations. Mendix has provided fix releases for the Mendix SAML module and recommends to update to the latest version.

The following versions of Siemens Mendix SAML are affected:

- **Mendix SAML (Mendix 10 compatible) vers:intdot/<4.2.3 (CVE-2026-80465)**
- **Mendix SAML (Mendix 11 compatible) vers:intdot/<4.2.3 (CVE-2026-80465)**
- **Mendix SAML (Mendix 9.24 compatible) vers:intdot/<3.6.27 (CVE-2026-80465)**

- **CVSS v3 8.7**
- **Vendor:** Siemens
- **Equipment:** Siemens Mendix SAML
- **Vulnerabilities:** Improper Verification of Cryptographic Signature

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-80465	High	Affected versions of the module do not properly validate the SAML response signature. This could allow unauthenticated remote attackers to hijack an account (session) in specific SSO configurations.

Remediation:

- Update to V3.6.27 or later version
- Update to V4.2.3 or later version
- Update to V4.2.3 or later version

Siemens Reyrolle 7SR5

Summary

Siemens Reyrolle 7SR5 Before V2.70 is affected by multiple vulnerabilities. Siemens has released a new version for Reyrolle 7SR5 and recommends to update to the latest version.

The following versions of Siemens Reyrolle 7SR5 are affected:

- **Reyrolle 7SR5 vers:intdot/<2.70 (CVE-2024-42384, CVE-2024-42385, CVE-2024-42386, CVE-2024-42391, CVE-2024-42392, CVE-2026-62645, CVE-2026-62646, CVE-2026-62647, CVE-2026-62648, CVE-2026-62649, CVE-2026-62650, CVE-2026-62652, CVE-2026-62653, CVE-2026-62654)**

- **CVSS v3 9.8**
- **Vendor:** Siemens
- **Equipment:** Siemens Reyrolle 7SR5
- **Vulnerabilities:** Integer Overflow or Wraparound, Improper Neutralization of Delimiters, Use of Out-of-range Pointer Offset, Missing Authentication for Critical Function, Insufficient Entropy, Improper Input Validation, Out-of-bounds Write, Allocation of Resources Without Limits or Throttling, Authentication Bypass Using an Alternate Path or Channel, Insertion of Sensitive Information Into Debugging Code, Download of Code Without Integrity Check

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2024-42384	High	Integer Overflow or Wraparound vulnerability in Cesanta Mongoose Web Server v7.14 allows an attacker to send an unexpected TLS packet and produce a segmentation fault on the application.
CVE-2024-42385	Medium	Improper Neutralization of Delimiters vulnerability in Cesanta Mongoose Web Server v7.14 allows to trigger an out-of-bound memory write if the PEM certificate contains unexpected characters.
CVE-2024-42386	High	Use of Out-of-range Pointer Offset vulnerability in Cesanta Mongoose Web Server v7.14 allows an attacker to send an unexpected TLS packet and produce a segmentation fault on the application.
CVE-2024-42391	Medium	Use of Out-of-range Pointer Offset vulnerability in Cesanta Mongoose Web Server v7.14 allows an attacker to send an unexpected TLS packet and force the application to read unintended heap memory space.
CVE-2024-42392	Medium	Improper Neutralization of Delimiters vulnerability in Cesanta Mongoose Web Server v7.14 allows to trigger an infinite loop bug if the input string contains unexpected characters.

CVE-2026-62645	Critical	Information is exposed through the web interface that can be used to calculate the current and past session ID numbers. This could allow an attacker to bypass the authentication and gain unauthorized access to the device.
CVE-2026-62646	High	A session identifier is generated using an algorithm with insufficient randomness, resulting in a token with low entropy that can be predicted or brute-forced within a feasible number of attempts. This could allow an unauthenticated remote attacker to derive valid session identifiers and bypass authentication.
CVE-2026-62647	High	A random number generator is used to generate security-relevant values (such as session identifiers used for authentication purposes) that is not initialized with a True Random Number Generator (TRNG), resulting in a predictable sequence of generated values. This could allow an unauthenticated remote attacker to more easily predict the generated values and impersonate a legitimate authenticated user, potentially gaining unauthorized access to the device.
CVE-2026-62648	High	The length of the URL component contained in pre-authenticated HTTP messages is not properly validated before appending additional data to it, resulting in an out-of-bounds write condition in memory. This could allow an unauthenticated remote attacker to crash the affected device, causing a reboot and resulting in a denial-of-service condition.
CVE-2026-62649	High	The web server does not properly limit or manage system resources when processing a high volume of concurrent HTTP requests. This could allow an unauthenticated remote attacker to cause the entire device to crash and reboot, resulting in a denial-of-service condition.
CVE-2026-62650	High	Server-side authorization checks in the web-based management interface are not properly enforced, allowing role-based access control (RBAC) restrictions to be bypassed through manipulation of request data. This could allow an authenticated, low-privileged remote attacker to escalate privileges to an administrative level.
CVE-2026-62652	Medium	The device firmware contains binaries from which debugging symbols have not been removed. This could allow an unauthenticated attacker with access to the publicly available firmware update files to more easily reverse engineer the device's firmware, facilitating the identification of further vulnerabilities.
CVE-2026-62653	Medium	The input received over a proprietary communication protocol that is exposed when the device is placed into a special firmware-update mode is not properly validated, resulting in a memory corruption condition. This could allow an unauthenticated attacker with physical access to the device to cause a crash and potentially execute arbitrary code on the device.
CVE-2026-62654	Medium	A special maintenance mode can be activated via a physical key sequence during device boot, in which the device downloads and executes program code from a network server without verifying its authenticity or integrity. This could allow an attacker with physical access to the device to upload and execute arbitrary, unsigned code.

Remediation:

- Update to V2.70 or later version

Schneider Electric SCADAPack x70 Products

Summary

Schneider Electric is aware of a vulnerability in its SCADAPack x70 products. The SCADAPack 47x, SCADAPack 47xi, SCADAPack 47xd, SCADAPack 470R and SCADAPack 57x products are Remote Terminal Units that provide communication capabilities for remote monitoring and control. Failure to apply the mitigations provided below may increase the risk of unauthorized access to RTU configuration through the Secure Lock functionality, potentially resulting in a loss of confidentiality.

The following versions of Schneider Electric SCADAPack x70 Products are affected:

- **SCADAPack 47x vers:all/* (CVE-2026-81861)**
- **SCADAPack 47xi vers:all/* (CVE-2026-81861)**
- **SCADAPack 47xd vers:all/* (CVE-2026-81861)**
- **SCADAPack 470R vers:all/* (CVE-2026-81861)**
- **SCADAPack 57x vers:all/* (CVE-2026-81861)**
- **SCADAPack 3xx vers:all/* (CVE-2026-81861)**
- **SCADAPack 32 vers:all/* (CVE-2026-81861)**

- **CVSS v3 6.5**
- **Vendor:** Schneider Electric
- **Equipment:** Schneider Electric SCADAPack x70 Products
- **Vulnerabilities:** Insufficiently Protected Credentials

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-81861	Medium	There is an insufficiently protected credentials vulnerability that could result in exposure of authentication information and unauthorized access to RTU functionality.

Remediation:

- Implement the Role-Based Access Control (RBAC) feature and follow the SCADAPack documentation sections Security Guidelines for Administrators and Working with Role-Based Access Control. RBAC is the recommended access control mechanism for SCADAPack 47x devices and should be used in place of the Secure Lock feature. The Secure Lock feature is legacy functionality retained for backward compatibility with existing deployments and should only be used where required to support legacy system requirements. Consult the SCADAPack Cybersecurity Guide, including the SCADAPack Hardening and Secured Communication sections. In addition, apply the following standard practices to reduce the risk of exploitation:
  - Configure network segmentation to restrict access between trusted and untrusted networks.
  - Enable and implement the RTU firewall service to restrict unauthorized access to device services and reduce the attack surface.

  Documentation available in [RemoteConnect and SCADAPack x70 Utilities | Schneider Electric].

- Ensure setup of network segmentation to restrict access between trusted and untrusted networks and implementation of the RTU Firewall Service to restrict unauthorized access to services. Consult the SCADAPack Cybersecurity Guide, including the SCADAPack Hardening and Secured Communication sections. In addition, implement all best practices referenced in the SCADAPack Cybersecurity Guide. Documentation available in RemoteConnect and SCADAPack x70 Utilities | Schneider Electric.
- For more information see the associated Schneider Electric security advisory SEVD-2026-251-03 Insufficiently Protected Credentials vulnerability on SCADAPack x70 Products PDF Version, CSAF Version.

mySCADA myPRO Manager

Summary

Successful exploitation of these vulnerabilities could allow an attacker to access privileged management functions or send arbitrary SMS messages through the connected GSM modem.

The following versions of mySCADA myPRO Manager are affected:

- **mySCADA myPRO Manager <=2.1 (CVE-2026-73807, CVE-2026-82567)**

- **CVSS v3 9.8**
- **Vendor:** mySCADA Technologies
- **Equipment:** mySCADA myPRO Manager
- **Vulnerabilities:** Missing Authorization, Missing Authentication for Critical Function

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-73807	Critical	The mySCADA myPRO Manager command API does not properly enforce authentication for privileged functions. An unauthenticated attacker with network access to the affected API could exploit this vulnerability to access privileged management functions.
CVE-2026-82567	Medium	The myPRO Manager notification gateway exposes an unauthenticated HTTP endpoint used to send SMS messages through a connected GSM modem. The endpoint is accessible over the network and does not require authentication before accepting a phone number and message from a request and sending the specified SMS message. An unauthenticated attacker with network access to the notification gateway could exploit this vulnerability to send arbitrary SMS messages through the connected modem.

Remediation:

- mySCADA Technologies has addressed these issues in Version 2.2 and recommends that users update to the latest version. Users are notified in mySCADA Pro Manager about the availability of a new version if the device is connected to the internet. Otherwise, users can download the mySCADA Pro Manager from the webpage.

Wärtsilä FOS-Onboard

Summary

Successful exploitation of these vulnerabilities could allow an attacker to deliver an unauthorized update, execute code, or extract credentials to allow the attacker to impersonate a privileged client.

The following versions of Wärtsilä FOS-Onboard are affected:

- **FOS-Onboard 5.07.0923.01 (CVE-2026-78225, CVE-2026-81855)**

- **CVSS v3 9.1**
- **Vendor:** Wärtsilä
- **Equipment:** Wärtsilä FOS-Onboard
- **Vulnerabilities:** Use of Hard-coded Cryptographic Key

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-78225	Critical	A hardcoded cryptographic server key vulnerability exists in the deployer-ng Update Controller component of Wärtsilä FOS-Onboard.
CVE-2026-81855	Critical	A hardcoded cryptographic client authentication key vulnerability exists in the robot testing framework component of Wärtsilä FOS-Onboard.

Remediation:

- Wärtsilä states that the vulnerabilities are not exploitable when the product is installed as recommended, and has developed a security patch. Users are also directed to contact Wärtsilä to obtain and install the patch. To obtain and install the latest patch, contact Wärtsilä.

Digital Watchdog VMAX DVR and NVR Product Lineups

Summary

Successful exploitation of these vulnerabilities could grant full administrative control of the device, allowing an attacker to view live and recorded surveillance, alter device configurations, and use the device as a network pivot point.

The following versions of Wärtsilä FOS-Onboard are affected:

- **VMAX A1 G4 DVRs vers:all/* (CVE-2026-68953, CVE-2026-66890, CVE-2026-68070, CVE-2026-68950, CVE-2026-66887, CVE-2026-66372)**
- **VMAX IP G4 NVRs vers:all/* (CVE-2026-68953, CVE-2026-66890, CVE-2026-68070, CVE-2026-68950, CVE-2026-66887, CVE-2026-66372)**
- **VMAX A1 PLUS vers:all/* (CVE-2026-68953, CVE-2026-66890, CVE-2026-68070, CVE-2026-68950, CVE-2026-66887, CVE-2026-66372)**
- **VA1G4 Recorder vers:all/* (CVE-2026-68953, CVE-2026-66890, CVE-2026-68070, CVE-2026-68950, CVE-2026-66887, CVE-2026-66372)**
- **VG4 Recorder vers:all/* (CVE-2026-68953, CVE-2026-66890, CVE-2026-68070, CVE-2026-68950, CVE-2026-66887, CVE-2026-66372)**

- **CVSS v3 9.6**
- **Vendor:** Digital Watchdog
- **Equipment:** Digital Watchdog VMAX DVR and NVR Product Lineups
- **Vulnerabilities:** Missing Authentication for Critical Function, Use of Hard-coded Credentials, Missing Authorization, Predictable Seed in Pseudo-Random Number Generator (PRNG)

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-68953	Medium	The affected products are vulnerable to an authentication bypass that allows unauthenticated remote attackers to disclose sensitive device information, including administrator credentials in plaintext, by sending crafted HTTP(S) requests.
CVE-2026-66890	Critical	The affected products use hard-coded credentials, which could allow remote access to files with root privileges where FTP is reachable.
CVE-2026-68070	High	The affected products are missing authentication for a critical function, which could allow an attacker to run as root and pass received bytes directly to a system command.
CVE-2026-68950	High	The affected products use hard-coded credentials, which could allow an attacker to run the ftpd service as root, providing remote root file access where FTP is reachable.
CVE-2026-66887	Critical	The affected products are missing authorization on state-changing CGIs and session checks are not performed.
CVE-2026-66372	Medium	The affected products use insufficiently random values, which allows web session tokens to be predictable, bounding token entropy to the seed space.

Remediation:

- Digital Watchdog has released updated firmware for the affected products. Users should download and install the updated firmware for their model.

References

https://www.cisa.gov/news-events/ics-advisories/icsa-26-258-08
https://www.cisa.gov/news-events/ics-advisories/icsa-26-258-07
https://www.cisa.gov/news-events/ics-advisories/icsa-26-258-06
https://www.cisa.gov/news-events/ics-advisories/icsa-26-258-05
https://www.cisa.gov/news-events/ics-advisories/icsa-26-258-04
https://www.cisa.gov/news-events/ics-advisories/icsa-26-258-03
https://www.cisa.gov/news-events/ics-advisories/icsa-26-258-02
https://www.cisa.gov/news-events/ics-advisories/icsa-26-258-01
https://sploitus.com/exploit?id=8330C8D8-76F2-5681-B9DB-1FEE71931C2C

CVEs

CVE-2026-88259
CVE-2026-84398

CVE-2026-84400
CVE-2026-81305
CVE-2026-85478
CVE-2026-85497
CVE-2026-81321
CVE-2026-58113
CVE-2026-80465
CVE-2024-42384
CVE-2024-42385
CVE-2024-42386
CVE-2024-42391
CVE-2024-42392
CVE-2026-62645
CVE-2026-62646
CVE-2026-62647
CVE-2026-62648
CVE-2026-62649
CVE-2026-62650
CVE-2026-62652
CVE-2026-62653
CVE-2026-62654
CVE-2026-81861
CVE-2026-73807
CVE-2026-82567
CVE-2026-78225
CVE-2026-81855
CVE-2026-68953
CVE-2026-66890
CVE-2026-68070
CVE-2026-68950
CVE-2026-66887
CVE-2026-66372

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com