Smarttech
YOUR 24/7 SECURITY PARTNER

Multiple Vulnerabilities in Industrial Control Systems - 21st October 2026

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	180
Authors	Mihai Butoi < mihai.butoi@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-10-21
Issue Date	2026-10-20

This document and any information therein are confidential property of Smarttech247 and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of Smarttech247, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. Smarttech247 retain the right to alter the document at any time unless a written statement to the contrary has been appended.

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 HMS Networks PEAK-System PCAN Windows drivers, Moxa AIG-302 ThingsPro Edge, Hitachi Energy MicroSCADA X SYS600, and Hitachi Energy RTU500 products. Successful exploitation of these vulnerabilities could allow attackers to cause denial-of-service conditions, crash Windows kernel components, disclose sensitive information and cryptographic key material, bypass authentication and authorization controls, compromise the confidentiality and integrity of communications, and potentially exploit memory-handling and input-validation weaknesses.

HMS Networks PEAK-System PCAN Windows drivers

Summary

Successful exploitation of these vulnerabilities could crash the Windows kernel.

The following versions of HMS Networks PEAK-System PCAN Windows drivers are affected:

- **PEAK-System Device Driver Setup <=5.1.2.1151 (CVE-2026-109576, CVE-2026-101103, CVE-2026-94188, CVE-2026-103672, CVE-2026-110322, CVE-2026-105960)**
- **PCAN Windows CAN device drivers <=5.1.2 (CVE-2026-109576, CVE-2026-101103, CVE-2026-94188, CVE-2026-103672, CVE-2026-110322, CVE-2026-105960)**

- **CVSS v3 7.1**
- **Vendor:** HMS Networks
- **Equipment:** PEAK-System Device Driver Setup
- **Vulnerabilities:** Out-of-bounds Write, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Improper Validation of Array Index, Untrusted Pointer Dereference, Improper Handling of Length Parameter Inconsistency

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-109576	Medium	The parser in PEAK-System PCAN driver correctly detected the malformed record, but the loop iterating the record list advanced its processed-bytes counter even when a record had been rejected as invalid.

CVE-2026-101103	Medium	The PEAK-System PCAN diagnostic call did not validate that the caller-supplied output buffer was large enough to hold the output record.
CVE-2026-94188	Medium	The copied source field in PEAK-System PCAN is attacker-influenced through the related file-device write path, and the caller can combine a small output allocation with controlled source bytes.
CVE-2026-103672	High	The PEAK-System PCAN parser indexes a length table using attacker-controlled DLC without enforcing DLC <= 0x0f, then copies attacker payload from record+0x1c into a fixed-size stack destination.
CVE-2026-110322	Medium	The PEAK-System PCAN type 0x4030 processing path fails to validate a selected/returned object pointer before dereferencing fixed fields during post-processing.
CVE-2026-105960	Medium	PEAK-System PCAN contains a vulnerable operation involving a variable-length receive-record copy. The driver uses a requested or queued record count without sufficiently capping the copy to the actual caller-supplied output length.

Recommended Practices:

- Upgrade HMS Networks PEAK-System PCAN Windows drivers to version 5.1.4, which addresses the reported vulnerabilities.
- Ensure control system devices and systems are not directly accessible from the internet.
- Place control system networks and remote devices behind firewalls and separate them from business networks.
- Use secure methods such as VPNs when remote access is required. Keep VPN software updated and ensure the connected devices are secure.
- Perform an impact analysis and risk assessment before implementing defensive measures.

Moxa AIG-302 ThingsPro Edge

Summary

Successful exploitation of these vulnerabilities could allow an attacker to obtain and disclose sensitive information.

The following versions of Moxa AIG-302 ThingsPro Edge are affected:

- **Moxa AIG-302 ThingsPro Edge firmware <=1.4.0 (CVE-2026-109812, CVE-2026-109813)**

- **CVSS v3 8.1**
- **Vendor:** Moxa
- **Equipment:** Moxa AIG-302 ThingsPro Edge firmware
- **Vulnerabilities:** Missing Authorization, Use of Hard-coded Cryptographic Key

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-109812	Medium	A missing authorization vulnerability exists in the internal API /api/v1/secrets/ for some of Moxa's industrial computing products. A privileged authenticated attacker with adjacent

		network access could exploit this vulnerability to access sensitive information, potentially resulting in the disclosure of confidential data, including cryptographic key material.
CVE-2026-109813	High	A hard-coded cryptographic key vulnerability exists in the /usr/bin/sysman for some of Moxa's industrial computing products. An unauthenticated attacker with adjacent network access could exploit the exposed private key material to compromise the confidentiality and integrity of communications.

Recommended Practices:

- Upgrade Moxa AIG-302 devices running firmware v1.4.0 or earlier to version v1.4.1.
- Ensure industrial computing devices are not directly accessible from the internet.
- Place industrial control systems behind firewalls and separate them from business networks.
- Use access control lists (ACLs) and allow connections only from trusted devices and networks.
- Use VPNs or other secure connections, and ensure remote-access software is updated.
- Apply strong authentication, role-based access control, and the principle of least privilege.
- Enable logging and monitor network traffic for unauthorized access or potential exploitation.
- Perform risk assessments before implementing defensive measures and regularly review device configurations.

Hitachi Energy MicroSCADA X SYS600 Product

Summary

Hitachi Energy is aware of multiple vulnerabilities that affect MicroSCADA X SYS600 product versions listed in this document. These vulnerabilities can be exploited to carry out various attacks on the product. Please refer to the Recommended Immediate Actions for information about the mitigation/remediation.

The following versions of Hitachi Energy MicroSCADA X SYS600 Product are affected:

- **MicroSCADA X SYS600 vers:MicroSCADA_X_SYS600/<=10.7, 10.8 (CVE-2026-9852, CVE-2026-9853, CVE-2026-9854, CVE-2026-9853)**

- **CVSS v3 7.8**
- **Vendor:** Hitachi Energy
- **Equipment:** MicroSCADA X SYS600
- **Vulnerabilities:** Improper Neutralization of Formula Elements in a CSV File, Incorrect Implementation of Authentication Algorithm

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-9852	Medium	A CSV injection vulnerability exists in SYS600. Injected malicious formulas can add or modify data to the spreadsheet, insert links, exfiltrate data, and in some cases, depending on how the user has their environment configured, execute malicious code on the user's machine. To exploit this issue attackers would need a way to create arbitrary log messages. This could be achieved through normal functionality via SCIL scripts, a log injection vulnerability, or via

		the SYS600 broker. This vulnerability affects all Windows users regardless of their privilege level who can run the Notify service and export the log.
CVE-2026-9853	High	A vulnerability exists in SYS600 which allows any user authenticated to the operating system of the server hosting the application to read and modify application objects without being authenticated to the SYS600 system itself. Only the SYS600 system users should be permitted to view and modify application objects.
CVE-2026-9854	High	A vulnerability exists in SYS600 RBAC mechanism where users having access to the engineering tools could elevate their privileges to administrator level on the underlying Windows host, granting themselves full control over the host machine.

Recommended Practices:

- Upgrade MicroSCADA X SYS600 to version 10.8 where applicable, and follow Hitachi Energy's specific remediation guidance for each vulnerability.
- Ensure control system devices and servers are not directly accessible from the internet.
- Place control system networks and remote devices behind firewalls and separate them from business networks.
- Use VPNs or other secure remote-access methods, keep VPN software updated, and secure the devices connected through them.
- Limit Windows logon rights on SYS600 servers to authorized personnel and service accounts, and review existing user accounts.
- Enforce appropriate password policies and access controls to prevent unauthorized access and privilege escalation.
- Scan portable computers and removable storage devices for malware before connecting them to control systems.
- Perform an impact analysis and risk assessment before deploying defensive measures or making system changes.

Hitachi Energy RTU500 Product

Summary

Hitachi Energy is aware of vulnerabilities that affect RTU500 product versions listed in this document. These vulnerabilities if exploited can have impact on confidentiality, integrity and availability of the product.

The following versions of Hitachi Energy RTU500 Product are affected:

- **RTU500 series CMU Firmware vers:RTU500_series_CMU_Firmware/>=13.5.1|<=13.5.4, vers:RTU500_series_CMU_Firmware/>=13.6.1|<=13.6.3, vers:RTU500_series_CMU_Firmware/>=13.7.1|<=13.7.8, vers:RTU500_series_CMU_Firmware/>=13.8.1|<=13.8.2, vers:RTU500_series_CMU_Firmware/>=12.7.1|<=12.7.7 (CVE-2026-17539, CVE-2026-28388, CVE-2026-6732, CVE-2026-6653, CVE-2026-6276, CVE-2026-9079, CVE-2026-11856, CVE-2026-8927, CVE-2026-8932, CVE-2026-17539, CVE-2026-28388, CVE-2026-6732, CVE-2026-6653, CVE-2026-6276, CVE-2026-9079, CVE-2026-11856, CVE-2026-8927, CVE-2026-8932, CVE-2026-17539, CVE-2026-28388, CVE-2026-6732, CVE-2026-6653, CVE-2026-6276, CVE-2026-9079, CVE-2026-11856, CVE-2026-8927, CVE-2026-8932, CVE-2026-17539, CVE-2026-28388, CVE-2026-6732, CVE-2026-6653, CVE-2026-6276, CVE-2026-9079, CVE-2026-11856, CVE-2026-8927, CVE-2026-**

8932, CVE-2026-17539, CVE-2026-28388, CVE-2026-6653)

- **CVSS v3 8.8**
- **Vendor:** Hitachi Energy
- **Equipment:** RTU500 series CMU Firmware
- **Vulnerabilities:** NULL Pointer Dereference, Access of Resource Using Incompatible Type ('Type Confusion'), Use After Free, Cleartext Transmission of Sensitive Information, Insufficiently Protected Credentials, Authentication Bypass by Capture-replay, Authentication Bypass by Primary Weakness

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-17539	Medium	RTU500 has a vulnerability, where high-load scenarios, such as sending GI requests at short intervals, may cause a NULL pointer dereference in the last entry of the enhanced message queue. This can cause a BCI_IEC104 fatal write error, resulting in connection interruption and restart, and ultimately a denial of service for bidirectional IEC 60870-5-104 communication.
CVE-2026-28388	High	A vulnerability exists in OpenSSL library component of RTU500 that is used for secure HTTPS access, authenticating and establishing encrypted communications with other devices. When processing a malformed delta CRL with a Delta CRL Indicator but no required CRL Number extension, OpenSSL may dereference a NULL pointer, causing a Denial of Service during X.509 certificate verification. Exploitation requires delta CRL processing to be enabled, a relevant freshest CRL condition to be present, and an attacker-supplied malformed CRL. The issue is limited to Denial of Service and cannot lead to code execution or memory disclosure.
CVE-2026-6732	High	The XML-based services used in RTU500 has a vulnerability while processing a specially crafted XSD-validated XML document may trigger a type confusion error in libxml2. An attacker could exploit this condition to cause a denial of service.
CVE-2026-6653	High	The XML-based services used in RTU500 has a vulnerability, where a use-after-free vulnerability in the xmlParseInternalSubset function of libxml2 may be triggered by processing specially crafted XML input. Improper handling of entity resolution can allow a remote attacker to cause a denial of service.
CVE-2026-6276	High	A vulnerability exists in the web-based management and services functions of RTU500 using libcurl library, when a custom `Host:` header is first set for an HTTP request and a second request is subsequently done using the same easy handle but without the custom `Host:` header set, the second request would use leaked stale information and pass on cookies meant for the first host in the second request.
CVE-2026-9079	Medium	A vulnerability exists in the web-based management and services functions of RTU500 using libcurl library. libcurl may fail to clear proxy authentication credentials when instructed to do so. As a result, stale credentials can be reused by subsequent transfers that should not access them, potentially exposing sensitive proxy authentication information.
CVE-2026-11856	High	A vulnerability exists in the web-based management and services functions of RTU500 using libcurl library. When the same libcurl handle is reused after a transfer to one HTTP origin using Digest authentication, libcurl may incorrectly send the Authorization

		header intended for the first origin to a second origin. This can disclose authentication information to an unintended host.
CVE-2026-8927	Medium	A vulnerability exists in the web-based management and services functions of RTU500 using libcurl library. When reusing a libcurl handle for sequential transfers with environment-variable proxy configuration, libcurl may fail to clear proxy authentication state between requests. This can leak the Proxy-Authorization header intended for one proxy to another proxy.
CVE-2026-8932	High	A vulnerability exists in the web-based management and services functions of RTU500 using libcurl library. libcurl may reuse an existing connection even after mTLS-related configuration options, especially client certificate or private key settings, have changed. This can bypass the intended authentication configuration and allow use of a connection that should no longer be reused.

Recommended Practices:

- Install the vendor-recommended firmware updates for affected Hitachi Energy RTU500 devices. The advisory identifies version 13.9.1 as a remediation version, with other version-specific fixes available or indicated for certain branches.
- Ensure control system devices and systems are not directly accessible from the internet.
- Place control system networks and remote devices behind firewalls and separate them from business networks.
- Use secure methods such as VPNs when remote access is required. Keep VPN software updated and ensure connected devices are secure.
- Prevent unauthorized personnel from directly accessing process control systems.
- Do not use process control systems for general web browsing, instant messaging, or email.
- Scan portable computers and removable storage devices for malware before connecting them to control systems.
- Apply appropriate password policies and secure account-management procedures.
- Perform an impact analysis and risk assessment before deploying defensive measures or changing operational systems.

References:

https://www.cisa.gov/news-events/ics-advisories/icsa-26-293-05
https://www.cisa.gov/news-events/ics-advisories/icsa-26-293-04
https://www.cisa.gov/news-events/ics-advisories/icsa-26-293-03
https://www.cisa.gov/news-events/ics-advisories/icsa-26-293-01

CVEs

CVE-2026-109576,
CVE-2026-101103,
CVE-2026-94188,
CVE-2026-103672,
CVE-2026-110322,
CVE-2026-105960,
CVE-2026-109812,
CVE-2026-109813,
CVE-2026-9852,
CVE-2026-9853,
CVE-2026-9854,
CVE-2026-17539,
CVE-2026-28388,
CVE-2026-6732,
CVE-2026-6653,
CVE-2026-6276,
CVE-2026-9079,
CVE-2026-11856,
CVE-2026-8927,
CVE-2026-8932.

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com