Smarttech
YOUR 24/7 SECURITY PARTNER

Multiple Vulnerabilities in Industrial Control Systems - 26th August 2026

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	146
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-08-26
Issue Date	2026-08-25

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

Overview

Multiple vulnerabilities have been identified in the following ICS-connected products: FURUNO FA-50 Class B AIS Transponder, Ebyte NE2-D11, Bendix EC80 Brake ECU, PayRange API, Siemens SIMATIC IoT2050 Advanced, Zoneminder, and Rently Smart Home. Successful exploitation of the vulnerabilities addressed in these advisories could result in unauthorized access, remote code execution, information disclosure, authentication bypass, session hijacking, unauthorized configuration changes, denial of service, and compromise of the confidentiality, integrity, and availability of affected systems.

FURUNO FA-50 Class B AIS Transponder

Summary

Successful exploitation of these vulnerabilities could allow an attacker to alter device settings.

The following versions of FURUNO FA-50 Class B AIS Transponder are affected:

- **FURUNO FA-50 Class B AIS Transponder vers:all/***

- **CVSS v3 9.1**
- **Vendor:** FURUNO ELECTRIC CO.,LTD.
- **Equipment:** FURUNO FA-50 Class B AIS Transponder
- **Vulnerabilities:** Use of Hard-coded Credentials, Missing Authentication for Critical Function

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-59769	Critical	An attacker, who knows the credentials and has access to the in-vessel network to which the device is connected to, may operate the settings screen using that credentials to alter the settings of the device.
CVE-2026-67578	High	Some configurations may be changed on the management screen without authentication.

Remediation:

- FURUNO ELECTRIC CO.,LTD. notes that production of this product ended in October 2020, and

software updates will no longer be provided. FURUNO recommends users do not connect the product directly to the internet. To prevent unauthorized access, the vessel on which the product is installed should be properly locked and managed.

Ebyte NE2-D11

Summary

Successful exploitation of these vulnerabilities could allow an attacker to gain unauthorized administrative access, disclose sensitive information, modify device configuration, hijack authenticated sessions, and disrupt device operation.

The following versions of Ebyte NE2-D11 are affected:

- **NE2-D11 Firmware FW-9167-0-11**

- **CVSS v3 9.8**
- **Vendor:** Ebyte
- **Equipment:** Ebyte NE2-D11
- **Vulnerabilities:** Missing Authentication for Critical Function, Cleartext Transmission of Sensitive Information, Insufficiently Protected Credentials, Use of Client-Side Authentication, Use of GET Request Method With Sensitive Query Strings, Cross-Site Request Forgery (CSRF), Improper Restriction of Excessive Authentication Attempts, Improper Restriction of Rendered UI Layers or Frames, Missing Authorization

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-73125	Critical	Ebyte device web management interface does not consistently enforce authentication before granting access to administrative functionality. An unauthenticated remote attacker could access sensitive configuration information, modify device settings, or disrupt availability.
CVE-2026-73809	High	A cleartext transmission of sensitive information vulnerability exists in certain Ebyte gateway products. The web management interface does not adequately protect sensitive communications using transport-layer encryption. An attacker with access to network traffic could intercept authentication or session-related information transmitted between a user and the affected device. Successful exploitation could result in disclosure of sensitive information and unauthorized access to device management functionality.
CVE-2026-73839	Medium	Administrative credentials may be exposed in plaintext within the Ebyte device's management interface, increasing the risk of credential compromise through visual or remote observation. This undermines the confidentiality of device access.
CVE-2026-71187	Critical	Ebyte device relies on client side authentication logic that can be reproduced by unauthenticated users. An attacker may generate valid authentication requests and bypass authentication to obtain administrative access to the device.
CVE-2026-76179	Critical	An improper protection of authentication tokens vulnerability exists in certain Ebyte gateway products. Authentication tokens used by the web management interface are insufficiently protected during client-side session handling, which may allow an attacker

		with access to exposed session information to obtain and reuse a valid token. Successful exploitation could allow an attacker to impersonate an authenticated user and gain unauthorized access to device management functionality.
CVE-2026-75814	High	Ebyte device does not adequately verify the origin or authenticity of requests submitted to the web management interface. An unauthenticated remote attacker could persuade an authenticated administrator to visit a crafted page, causing unauthorized configuration changes or a disruption of device availability.
CVE-2026-76940	High	The affected Ebyte device does not restrict repeated authentication attempts through rate limiting or account lockout mechanisms. This could allow an attacker to perform automated authentication attacks against deployments that rely on password based authentication.
CVE-2026-75548	Medium	The affected Ebyte device web management interface does not restrict the interface from being rendered within an external frame. An unauthenticated remote attacker could use a crafted webpage to mislead an authenticated administrator into initiating unintended configuration changes or disruptive actions.
CVE-2026-75813	High	Certain configuration endpoints may lack proper server-side authorization checks, allowing unauthorized users to access or modify sensitive device settings. This could result in full compromise of device functionality.
CVE-2026-76945	High	The affected Ebyte device relies on client-managed authentication tokens without sufficient server-side validation. An attacker may replay or manipulate authentication tokens to gain unauthorized access to administrative functionality.
CVE-2026-69658	Critical	MQTT credentials and control traffic are transmitted in cleartext, exposing sensitive information to network-level attackers. This may enable unauthorized device impersonation and disruption of messaging functions.

Remediation:

- Ebyte acknowledged receipt of the reported vulnerabilities and indicated that a patch was under development. However, the vendor has not responded to subsequent requests for coordination, and CISA has not been informed of the status or availability of the patch. Users are encouraged to reach out to Ebyte for more information.

Bendix EC80 Brake ECU

Summary

Successful exploitation of these vulnerabilities could allow an attacker to cause the loss of ABS functions, steering assist, speedometer, shifting capabilities, or disable automatic traction control.

The following versions of Bendix EC80 Brake ECU are affected:

- **EC80ESP+ J1708 Z228999**
- **EC80ESP+ 6S/6M Z228999**
- **EC80ESP+ PLC Z228999**
- **EC80ESP+ 2nd CAN Z228999**
- **EC80ESP+ Integrated TPMS Z228999**
- **EC80ESP 6S/6M Z266494**

- **EC80ESP PLC Z266494**
- **EC80ESP 2nd CAN Z266494**
- **EC80ESP CAN Gateway Z266494**
- **EC80ESP 4S/4M Z286098**
- **EC80ESP PLC Z286098**

- **CVSS v3 7.5**
- **Vendor:** Bendix
- **Equipment:** Bendix EC80 Brake ECU
- **Vulnerabilities:** Stack-based Buffer Overflow, Out-of-bounds Write, Use of Hard-coded Credentials

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-67560	High	The affected product is vulnerable to a stack-based buffer overflow, which may allow an attacker to crash the ECU. A crafted payload can then be used to remotely execute arbitrary code or inject arbitrary CAN bus traffic. This could cause the loss of the ABS function, steering assist, speedometer, and shifting.
CVE-2026-68967	Medium	The affected product is vulnerable to an out-of-bounds write, which could allow an attacker to deliver a payload that could establish an arbitrary write primitive, which could crash the ECU.
CVE-2026-71396	Medium	The affected product uses hard-coded credentials, which could allow an attacker to disable automatic traction control.

Remediation:

- Bendix recommends users update their firmware to the most recent firmware version releases. Users that need more help should contact Bendix directly at info@Bendix.com.
- EC80ESP+ J1708: Z228999 users should update their firmware to version Z300822.
- EC80ESP+ 6S/6M: Z228999 users should update their firmware to version Z300822.
- EC80ESP+ PLC: Z228999 users should update their firmware to version Z300822.
- EC80ESP+ 2nd CAN: Z228999 users should update their firmware to version Z300822.
- EC80ESP+ Integrated TPMS: Z228999 users should update their firmware to version Z300822.
- EC80ESP 6S/6M: Z266494 users should update their firmware to version Z302578.
- EC80ESP PLC: Z266494 users should update their firmware to version Z302578.
- EC80ESP 2nd CAN: Z266494 users should update their firmware to version Z302578.
- EC80ESP CAN Gateway: Z266494 users should update their firmware to version Z302578.
- EC80ESP 4S/4M: Z286098 users should update their firmware to version Z302579.
- EC80ESP PLC: Z286098 users should update their firmware to version Z302579.

PayRange API

Summary

Successful exploitation of this vulnerability could allow a remote, authenticated or unauthenticated attacker to disclose sensitive information, arbitrarily modify the device to cause a denial of service, or alter a devices displayed image.

The following versions of PayRange API are affected:

- **PayRange API vers:all/***

- **CVSS v3 8.8**
- **Vendor:** PayRange
- **Equipment:** PayRange API
- **Vulnerabilities:** Missing Authorization

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-18965	High	The affected product is missing proper authorization on management endpoints, which allows verbose details of every device on the PayRange network to be publicly accessible, with or without an account.

Remediation:

- PayRange has not responded to requests to work with CISA to mitigate this vulnerability. Users of PayRange devices are invited to contact PayRange customer support at support@payrange.com for additional information.

Siemens SIMATIC IoT2050 Advanced

Summary

SIMATIC IoT2050 Advanced devices running Industrial OS with Node-RED installed contain a missing authentication vulnerability in the Node-RED HTTP interface that could allow an unauthenticated remote attacker to create malicious flows and execute arbitrary code on the underlying server with maximum privileges. Siemens has released a new version for SIMATIC IoT2050 Advanced and strongly recommends to update to the latest version.

The following versions of Siemens SIMATIC IoT2050 Advanced are affected:

- **SIMATIC IoT2050 Advanced (6ES7647-0BA00-1YA2) vers:intdot/<4.3.4.1**

- **CVSS v3 10**
- **Vendor:** Siemens
- **Equipment:** Siemens SIMATIC IoT2050 Advanced
- **Vulnerabilities:** Missing Authentication for Critical Function

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-58115	Critical	Affected devices do not enforce authentication on the Node-RED

		HTTP interface, allowing unauthenticated access to programming nodes that are capable of executing system commands on the server. This could allow an unauthenticated remote attacker to create malicious flows through the HTTP interface in order to execute arbitrary code on the underlying server with maximum privileges.

Remediation:

- Harden the Node-RED installation (see Node-RED User Guide)
- Uninstall Node-RED
- Update to V4.3.4.1 or later version

Zoneminder

Summary

Successful exploitation of this vulnerability could result in full Remote Code Execution (RCE) as the web server user.

The following versions of Zoneminder are affected:

- **Zoneminder 1.37.48|1.38.3**

- **CVSS v3 8.8**
- **Vendor:** Zoneminder
- **Equipment:** Zoneminder
- **Vulnerabilities:** Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-76060	High	An authenticated OS Command Injection vulnerability exists in ZoneMinder's event export functionality. The exportFile HTTP request parameter is passed unsanitized into a shell command executed via PHP's exec(), allowing any authenticated user with View Events permission to execute arbitrary operating system commands on the server.

Remediation:

- Zoneminder recommends upgrading to version 1.38.3 or later by downloading the installer for your system at: https://zoneminder.com/downloads.
- Users may also get the source code from Zoneminder's Github: https://github.com/ZoneMinder/zoneminder.
- For more details refer to Zoneminder's security advisories at: https://github.com/ZoneMinder/zoneminder/security/advisories/GHSA-88m4-hrgp-m9v3.

Rently Smart Home

Summary

Successful exploitation of this vulnerability could allow an attacker to access sensitive information and override user permissions.

The following versions of Rently Smart Home are affected:

- **Smart Home <=20.1.0**

- **CVSS v3 8.1**
- **Vendor:** Rently
- **Equipment:** Rently Smart Home
- **Vulnerabilities:** Insufficiently Protected Credentials

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-75960	High	Rently Smart Home versions 20.1.0 and prior are vulnerable to an Insufficiently Protected Credentials vulnerability. This could allow an attacker to retrieve pins including the Master Pin, overriding standard user permissions.

Remediation:

- Rently has patched this vulnerability in late June. No user action is required.

References

https://www.cisa.gov/news-events/ics-advisories/icsa-26-237-07
https://www.cisa.gov/news-events/ics-advisories/icsa-26-237-06
https://www.cisa.gov/news-events/ics-advisories/icsa-26-237-05
https://www.cisa.gov/news-events/ics-advisories/icsa-26-237-04
https://www.cisa.gov/news-events/ics-advisories/icsa-26-237-03
https://www.cisa.gov/news-events/ics-advisories/icsa-26-237-02
https://www.cisa.gov/news-events/ics-advisories/icsa-26-237-01
https://www.scriptkittens.com/blog/two-sinks-one-shell

CVEs

CVE-2026-75960
CVE-2026-76060
CVE-2026-58115
CVE-2026-18965
CVE-2026-67560
CVE-2026-68967
CVE-2026-71396
CVE-2026-73125
CVE-2026-73809
CVE-2026-73839
CVE-2026-71187
CVE-2026-76179
CVE-2026-75814
CVE-2026-76940
CVE-2026-75548
CVE-2026-75813
CVE-2026-76945
CVE-2026-69658
CVE-2026-59769
CVE-2026-67578

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com