Smarttech
YOUR 24/7 SECURITY PARTNER

Multiple Vulnerabilities in Industrial Control Systems - 15th July 2026

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	118
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-07-15
Issue Date	2026-07-15

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: **ABB Advant Master Online Builder**, **ABB Ability Edgenius, ABB T-MAC Plus**, and **Rockwell Automation 1715-AENTR EtherNet/IP Adapter**. Successful exploitation of these vulnerabilities could lead to unauthorized code execution, privilege escalation, sensitive information disclosure, unauthorized administrative access, cross-site scripting (XSS), denial-of-service conditions, and compromise of affected devices.

ABB Advant Master Online Builder

Summary

ABB became aware of vulnerability in the products versions listed as affected in the advisory, where an incorrect version of Online Builder (ONB) was included in the media.

The following versions of ABB Advant Master Online Builder are affected:

- **Control Builder A <=1.4/4 (CVE-2025-13162)**
- **800xA for Advant Master <=6.0.3-1, <=6.1.1-1, 6.1.1-3, 6.2.0-1 (CVE-2025-13162, CVE-2025-13162, CVE-2025-13162, CVE-2025-13162)**

- **CVSS v3 4.4**
- **Vendor:** ABB
- **Equipment:** ABB Advant Master Online Builder
- **Vulnerabilities:** Uncontrolled Search Path Element

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2025-13162	Medium	The application improperly handles the search path for loading DLL´s, potentially allowing unauthorized libraries from untrusted directories. An attacker who obtains the necessary access could exploit the vulnerability leading to unauthorized code execution and compromising system integrity.

Remediation:

- ABB has investigated the vulnerability and remediated it in the newly released

versions. The vulnerability has been resolved in the product versions listed as fixed in the advisory. - Version 6.1.1-2 does not contain this vulnerability and therefore no update is required. The vulnerability was again introduced in 6.1.1-3 when an older ONB version was included in the release media. - Version 6.1.1-4 do not contain this vulnerability but present version 6.1.1-3 by 800xA System Installer and System Configuration Console (SCC). Version 6.1.1-4 is therefore withdrawn. - Version 6.2.0-2 do not contain this vulnerability but present version 6.2.0-1 by 800xA System Installer and System Configuration Console (SCC). Version 6.2.0-2 is therefore withdrawn. ABB recommends that customers apply the update at their earliest convenience. - Control Builder A: It is recommended to update Control Builder A to version 1.4/5 or later. - 800xA for Advant Master: - Versions 6.0.3-1 and earlier, - Versions 6.1.1-1 and earlier, - Versions 6.1.1-2, 6.1.1-3, and 6.1.1-4 should be updated to version 6.1.1-5 or later. - 800xA for Advant Master: - Versions 6.2.0-1 and 6.2.0-2 should be updated to version 6.2.0-3 or later.

- Since it is required that the attacker has access to the system, it is important that all users that have access to the system are managed as recommended by ABB guidelines. - Allow only authorized users to log on to the system and enforce strong passwords that are changed regularly. - Restrict temporary connection of portable computers, USB memory devices and other removable data carriers. Computers that can be physically accessed by regular users should have ports for removable data carriers disabled or at least managed to only allow intended device types.
- The recommendation is to upgrade to a version where the vulnerability is corrected. If an upgrade Is not possible and a workaround is needed, contact ABB Support.

ABB Ability Edgenius

Summary

ABB is aware of public reports of a vulnerability CVE-2026-31431 (Copy Fail) in the product versions listed as affected in the advisory. An update is available that resolves a publicly reported vulnerability. CVE-2026-31431 (Copy Fail) is a Linux kernel vulnerability that may allow a locally authenticated user or compromised container workload to gain elevated (root) privileges on affected systems. Once root access is obtained, the attacker can effectively gain complete control of the system

The following versions of ABB Ability Edgenius are affected:

- **Ability Edgenius >=3.2.0.0|<3.2.4.1 installed on ABB Ability Edgenius Gateway - bE100, >=3.2.0.0|<3.2.4.1 installed on ABB Ability Edgenius Gateway - E3100C, >=3.2.0.0|<3.2.4.1 installed on ABB Ability Edgenius Server - vE1000 (CVE-2026-31431, CVE-2026-31431, CVE-2026-31431)**

- **CVSS v3 7.8**
- **Vendor:** ABB
- **Equipment:** ABB Ability Edgenius
- **Vulnerabilities:** Incorrect Resource Transfer Between Spheres

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-31431	High	CVE-2026-31431 (Copy Fail) is a Linux kernel vulnerability that

		may allow a locally authenticated user or compromised container workload to gain elevated (root) privileges on affected systems. The issue originates in the Linux kernel's cryptographic subsystem and impacts kernels used by most major Linux distributions released since 2017. Successful exploitation requires local code execution, however, in shared, containerized, or multi-tenant environments this may increase the security risk

Remediation:

- The problem is corrected in the following product versions: - Edgenius 3.2.4.1 ABB recommends that customers apply the update at earliest convenience.
- Mitigating factors describe conditions and circumstances that make an attack that exploits the vulnerability difficult or less likely to succeed. Refer to section General security recommendations for further advise on how to keep your system secure. Recommended mitigation factors - Limit access to ssh or cockpit - By default, no additional lower privilege users are present on Edgenius installations

ABB T-MAC Plus

Summary

ABB became aware of vulnerability in the products versions listed as affected in the advisory. An update is available that resolves the reported vulnerabilities. An attacker who successfully exploited any of these vulnerabilities could potentially compromise the system in different ways.

The following versions of ABB T-MAC Plus are affected:

- **T-MAC Plus 4.0-24 (CVE-2025-14771, CVE-2025-14772, CVE-2025-14773, CVE-2025-14774)**

- **CVSS v3 9.9**
- **Vendor:** ABB
- **Equipment:** ABB T-MAC Plus
- **Vulnerabilities:** Files or Directories Accessible to External Parties, Authorization Bypass Through User-Controlled Key, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Incorrect Authorization

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2025-14771	Critical	File Disclosure in ABB T-MAC Plus web application allows authenticated users to exfiltrate files containing sensitive information via crafted HTTP GET request.
CVE-2025-14772	High	Broken access controls in ABB T-MAC Plus web application allows unprivileged users to performs administrative operations
CVE-2025-14773	High	Stored Cross-Site Scripting (XSS) in ABB T-MAC Plus web application allows authenticated users to execute arbitrary HTML or JavaScript code on victims browser.
CVE-2025-14774	High	Insecure network protocol in ABB T-MAC Plus allows unauthenticated attackers to perform a denial-of-service (DoS) of the Card Reader service.

Remediation:

- ABB has investigated these vulnerabilities to provide adequate protection to customers. The problem is corrected in the following product versions: T-MAC Plus version 4.0-25 ABB recommends that customers apply the update at earliest convenience.
- If a malicious actor gains physical access to a serial device, disables it, connects a malicious device with same IP address, and sends a specially crafted message, the service responsible for communicating with the device will be blocked until a manual restart is performed. New T-MAC Plus version 4.0-25 will correct the vulnerability.
- Workarounds are specific measures that a user can take to help block an attack, for example, temporarily disabling the vulnerable feature may remove the exposure with well-known impact on functionality. ABB has tested the following workarounds. Although these workarounds will not correct the underlying vulnerability, they can help block known attack vectors. When a workaround reduces functionality, this is identified below as "Impact of workaround".

Rockwell Automation 1715-AENTR EtherNet/IP Adapter

Summary

Successful exploitation of this vulnerability could allow an attacker to read or delete files, stop tasks, modify memory, and change I/O states, potentially impacting the confidentiality, integrity, and availability of the device.

The following versions of Rockwell Automation 1715-AENTR EtherNet/IP Adapter are affected:

- **1715-AENTR EtherNet/IP Adapter <=3.003 (CVE-2026-10577)**

- **CVSS v3 10**
- **Vendor:** Rockwell Automation
- **Equipment:** Rockwell Automation 1715-AENTR EtherNet/IP Adapter
- **Vulnerabilities:** Missing Authentication for Critical Function

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-10577	Critical	A security issue exists within the 1715-AENTR EtherNet/IP Adapter. The affected product exposes a network-accessible debug port that does not enforce proper privilege controls, allowing unauthenticated remote access to intrusive command-line interface (CLI) commands. If exploited, a threat actor could read or delete files, stop tasks, modify memory, and change I/O states, potentially impacting the confidentiality, integrity, and availability of the device.

Remediation:

- Rockwell Automation recommends that users update to 1715-AENTR EtherNet/IP Adapter version 3.011 and later.
- Rockwell Automation recommends users of the affected software who are not able to upgrade to one of the corrected versions should use their security best practices.

References

https://www.cisa.gov/news-events/ics-advisories/icsa-26-195-01
https://www.cisa.gov/news-events/ics-advisories/icsa-26-195-02
https://www.cisa.gov/news-events/ics-advisories/icsa-26-195-03
https://www.cisa.gov/news-events/ics-advisories/icsa-26-195-04

CVEs

CVE-2025-13162
CVE-2026-31431
CVE-2025-14771
CVE-2025-14772
CVE-2025-14773
CVE-2025-14774
CVE-2026-10577

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com