Smarttech
YOUR 24/7 SECURITY PARTNER

Multiple Vulnerabilities in ABB Products - 13th May 2026

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	72
Authors	Bojian Denis < denis.bojian@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-05-13
Issue Date	2026-05-12

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 Industrial Control Systems / ICS-connected products: **ABB WebPro SNMP Card PowerValue, ABB AC500 V3, ABB Automation Builder Gateway for Windows, ABB AC500 V3 Stack Buffer Overflow in Cryptographic Message Syntax.** Successful exploitation of these vulnerabilities across the affected ABB products could enable attackers to bypass authentication and user management controls, perform unauthorized access to device functions, and manipulate or exfiltrate sensitive configuration data, including cryptographic certificates and keys. Depending on the component and flaw, attackers may also be able to scan and discover PLCs on affected networks, disrupt device availability through denial-of-service conditions, maintain or hijack active sessions, and in certain cases modify or inject data into industrial processes. In the most severe scenarios, exploitation could potentially lead to remote code execution on affected controllers or services, resulting in a full compromise of confidentiality, integrity, and availability within industrial control system environments.

ABB WebPro SNMP Card PowerValue

Summary

These vulnerabilities were internally discovered by ABB relating to multiple security flaws in the WebPro SNMP Card PowerValue firmware used for remote UPS monitoring and management. ABB became aware of multiple internally discovered vulnerabilities in the WebPro SNMP Card PowerValue. Depending upon the vulnerability, an attacker with access to the local network who successfully exploited these vulnerabilities could disrupt device availability or take control of the target device.

The following versions of ABB WebPro SNMP Card PowerValue are affected:

- **ABB WebPro SNMP Card PowerValue through version 1.1.8.K**
- **ABB WebPro SNMP Card PowerValue UL through version 1.1.8.K**
- **CVSS v3 8.8**
- **Vendor:** ABB
- **Equipment:** WebPro SNMP Card PowerValue / PowerValue UL
- **Vulnerabilities:** Improper Input Validation (DoS), Authentication Algorithm Bypass, Insufficient Session Expiration

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2025-4675	High	An Improper Check for Unusual or Exceptional Conditions vulnerability. The Modbus (slave) protocol was implemented incorrectly in the device on port 502, allowing an attacker with adjacent network access to cause a denial-of-service condition by sending specially crafted messages. No authentication is required to exploit this vulnerability. Impact is limited to availability.
CVE-2025-4676	High	An Incorrect Implementation of Authentication Algorithm vulnerability. Improper implementation of authentication mechanisms may allow an attacker on an adjacent network, with user interaction, to bypass security controls and impact the confidentiality, integrity, and availability of downstream connected systems.
CVE-2025-4677	High	An Insufficient Session Expiration vulnerability. The device fails to properly invalidate user sessions after inactivity or explicit logout, allowing session tokens to remain valid beyond their intended lifespan. An attacker on an adjacent network, without authentication, can exploit this to cause a denial-of-service condition affecting device availability.

Remediation: ABB strongly advises customers to update to the latest firmware, noting that WebPro SNMP Card PowerValue v1.1.8.p includes fixes for all previously listed vulnerabilities; at the time the advisory was issued, none of the vulnerabilities had been publicly disclosed and ABB had received no reports of active exploitation. ABB recommends immediately updating all affected WebPro SNMP Card PowerValue and PowerValue UL devices to firmware version v1.1.8.p or later, ensuring that network systems are physically protected and not directly connected to the Internet or any untrusted network, separating affected devices from other networks using a firewall with a minimal number of exposed ports, and, when remote access is required, using secure methods such as VPNs that are kept updated to the most recent version available.

ABB AC500 V3

Summary

These vulnerabilities were publicly reported and internally validated by ABB relating to multiple security flaws in the AC500 V3 Programmable Logic Controller (PLC) firmware. An attacker who successfully exploited these vulnerabilities could bypass the user management and read visualization files read and write certificates and keys), or cause a denial-of-service (DoS).

The following versions of ABB AC500 V3are affected:

- **All AC500 V3 products (PM5xxx) with firmware version earlier than 3.9.0**
- **AC500 V3 firmware versions: <3.9.0, 3.9.0**

- **CVSS v3 8.3**
- **Vendor: ABB**
- **Equipment: AC500 V3 PLC (PM5xxx series)**
- **Vulnerabilities: Forced Browsing / Authorization Bypass, Incorrect**

Permission Assignment for Critical Resource, NULL Pointer Dereference (DoS)

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2025-2595	Medium	Visualization user management bypass in WebVisu. An unauthenticated remote attacker can bypass the built-in user management and read visualization files by means of forced browsing. The exposed files, accessible via a web browser, contain only static visualization data such as text lists, icons or images, but no live data from the controlled system.
CVE-2025-41659	High	Exposed PKI folder. A vulnerability in the runtime system allows low-privileged remote attackers to access the PKI folder via CODESYS protocol, enabling them to read and write certificates and keys. This exposes sensitive cryptographic data and allows unauthorized certificates to be trusted. However, all services remain available; only certificate-based encryption and signing features are affected. The issue affects systems using the optional CmpOpenSSL component for cryptographic operations
CVE-2025-41691	High	NULL Pointer Dereference. A vulnerability in the runtime system's CmpDevice component allows unauthenticated attackers to cause a denial-of-service (DoS) via specially crafted communication requests. The issue is triggered by a NULL pointer dereference and also affects systems when outdated clients attempt to log in.

Remediations: The problem is corrected in AC500 V3 firmware version 3.9.0, and ABB recommends that customers apply the update at the earliest convenience; this firmware version is released for all AC500 V3 PLC types and is available through Automation Builder 2.9.0, which can be downloaded from ABB Automation Builder Software Download. ABB states that no workarounds are available and notes that, at the time the advisory was issued, the vulnerabilities had been publicly disclosed but there were no reports of active exploitation; the company further recommends isolating special-purpose networks (such as automation systems) and remote devices behind firewalls and separating them from general-purpose networks, installing physical controls to prevent unauthorized access to devices, components, peripheral equipment, and networks, minimizing network exposure so that applications and endpoints are not accessible from the Internet unless specifically designed for such exposure, keeping all nodes up to date with the latest software, operating system, firmware patches, and security solutions, and using secure remote access methods such as updated Virtual Private Networks (VPNs) when remote connectivity is required. Additionally, CISA recommends performing proper impact analysis and risk assessments before deploying defensive measures and following established internal procedures to report any suspected malicious activity for tracking and correlation.

ABB Automation Builder Gateway for Windows

Summary

The issue affects the ABB Automation Builder Gateway for Windows, which is used as a

communication channel between clients and ABB AC500 PLCs. By default, the gateway listens on all available network interfaces and can be accessed remotely. If improperly configured, this behavior may allow unauthenticated attackers to scan for PLCs within the network. Although built-in PLC user management typically prevents direct access, disabling user management or using insecure configurations may increase exposure. An attacker who successfully exploits this vulnerability could scan for connected PLCs and access restricted PLC networks (depending on configuration). The vulnerability results from an insecure default configuration in the gateway service.

The following versions of ABB Automation Builder Gateway for Windows are affected:

- **Automation Builder versions earlier than 2.9.0**
- **Automation Builder 2.9.0 (initial release prior to security fix)**

- **CVSS v3.1 5.3**
- **Vendor: ABB**
- **Equipment: Communication gateway for ABB AC500 PLCs**
- **Vulnerabilities: Initialization of a Resource with an Insecure Default**

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2024-41975	Medium	The CODESYS Gateway serves as a communication channel for various clients to CODESYS runtimes. By default, the CODESYS Gateway listens on all available network adapters on port 1217 and can therefore be accessed remotely. However, remote access to the CODESYS Gateway is only required in certain network configurations. Since the CODESYS Gateway is usually accessed locally, many users are unaware of this remote access option, which can enable scanning of and access to restricted PLC networks. Unauthenticated attackers can therefore search for PLCs, but the user management of the PLCs prevents the actual access to the PLCs — unless it is disabled.

Remediations:
Update CODESYS Edge Gateway for Windows and CODESYS Gateway for Windows to version 3.5.21.0, which is available as part of Automation Builder 2.9.0, and ABB recommends that customers apply the update at their earliest convenience; when the advisory was issued, the vulnerability had already been publicly disclosed, and ABB had received no reports of active exploitation at the time of original publication. ABB further recommends isolating special-purpose networks (such as automation systems) and remote devices behind firewalls and separating them from general-purpose networks, installing physical controls to prevent unauthorized access to devices, components, peripheral equipment, and networks, minimizing network exposure so that applications and endpoints are not accessible from the Internet unless specifically required, ensuring all nodes remain up to date with the latest software, operating system, firmware patches, antivirus, and firewall solutions, and using secure remote access methods such as Virtual Private Networks (VPNs) when needed, keeping them updated to the most current version available.

ABB AC500 V3 Stack Buffer Overflow in Cryptographic Message Syntax

Summary

This vulnerability was publicly reported and relates to a stack buffer overflow in the OpenSSL

library's Cryptographic Message Syntax parsing code, which is incorporated into the ABB AC500 V3 PLC firmware. ABB became aware of a vulnerability in the product versions listed as affected in the advisory. An update is available that resolves this publicly reported vulnerability. An attacker who successfully exploited this vulnerability could cause a crash, denial-of-service, or potentially remote code execution.

The following versions of ABB Ability OPTIMAX are affected:

- **AC500 V3 PM5xxx firmware versions 3.9.0 and 3.9.0_HF1**

- **CVSS v3 9.8**
- **Vendor: ABB**
- **Equipment: AC500 V3 PLC (PM5xxx series)**
- **Vulnerabilities:** Stack-based Buffer Overflow in OpenSSL CMS Parsing

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2025-15467	Critical	When parsing CMS (Auth)EnvelopedData structures that use AEAD ciphers such as AES-GCM, the IV (Initialization Vector) encoded in the ASN.1 parameters is copied into a fixed-size stack buffer without verifying that its length fits the destination. An attacker can supply a crafted CMS message with an oversized IV, causing a stack-based out-of-bounds write before any authentication or tag verification occurs. Because the overflow occurs prior to authentication, no valid key material is required to trigger it. While exploitability to remote code execution depends on platform and toolchain mitigations, the stack-based write primitive represents a severe risk.

Remediations:
The problem is corrected in AC500 V3 firmware version 3.9.0 HF1, and ABB recommends that customers apply the update at the earliest convenience, noting that AC500 V3 firmware version 3.9.0 is still listed as affected and that users must specifically upgrade to 3.9.0 HF1 (Hotfix 1) to fully resolve the vulnerability; when the advisory was issued, the vulnerability had already been publicly disclosed, and ABB had received no reports of active exploitation at the time of original publication. ABB further recommends isolating special-purpose networks (such as automation systems) and remote devices behind firewalls and separating them from general-purpose networks, installing physical controls to prevent unauthorized access to devices, components, peripheral equipment, and networks, minimizing network exposure so that applications and endpoints are not accessible from the Internet unless strictly required, keeping all nodes continuously updated with the latest software, operating system, firmware patches, antivirus, and firewall protections, and using secure remote access methods such as Virtual Private Networks (VPNs) when necessary, ensuring they are kept up to date.

References

https://www.cisa.gov/news-events/ics-advisories/icsa-26-132-06
https://www.cisa.gov/news-events/ics-advisories/icsa-26-132-03
https://www.cisa.gov/news-events/ics-advisories/icsa-26-132-04
https://www.cisa.gov/news-events/ics-advisories/icsa-26-132-05

CVEs

CVE-2025-4675
CVE-2025-4676
CVE-2025-4677
CVE-2025-2595
CVE-2025-41659
CVE-2025-41691
CVE-2024-41975
CVE-2025-15467


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com