DOCUMENT ID: 3ADR011536
REVISION: A
DATE: 2026-03-12

CYBER SECURITY ADVISORY

AC500 V3
Stack buffer overflow in Cryptographic Message Syntax

CVE ID: CVE-2025-15467

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

Purpose

ABB has a rigorous internal cyber security continuous improvement process which involves regular testing with industry leading tools and periodic assessments to identify potential product issues. Occasionally an issue is determined to be a design or coding flaw with implications that may impact product cyber security.

When a potential product vulnerability is identified or reported, ABB immediately initiates our vulnerability handling process. This entails validating if the issue is in fact a product issue, identifying root causes, determining what related products may be impacted, developing a remediation, and notifying end users and governmental organizations.

The resulting Cyber Security Advisory intends to notify customers of the vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk as much as possible. The release of a Cyber Security Advisory should not be misconstrued as an affirmation or indication of an active threat or ongoing campaign targeting the products mentioned here. If ABB is aware of any specific threats, it will be clearly mentioned in the communication.

The publication of this Cyber Security Advisory is an example of ABB's commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information which is essential to help ensure our customers are fully informed.

Affected products

All AC500 V3 products (PM5xxx) with firmware version 3.9.0 are affected by this vulnerability.

Other firmware versions than 3.9.0 are not affected.

Vulnerability ID

CVE-2025-15467

Summary

An update is available that resolves publicly reported vulnerability in the product version listed above.

An attacker who successfully exploited these vulnerabilities could cause a crash, denial-of-service (DoS), or potentially remote code execution.

Recommended immediate actions

The problem is corrected in the following product version:

AC500 V3 firmware version 3.9.0 HF1

ABB recommends that customers apply the update at earliest convenience. This firmware version is released for all AC500 V3 PLC types and available for download from the ABB library.

Vulnerability severity and details

Multiple vulnerabilities exist in the AC500 V3 included in the product version listed above. For details, please refer to the subchapters for the different CVEs.

A vulnerability exists in the OpenSSL component included in the product version listed above. An attacker could exploit the vulnerability by sending a specially crafted message to the system node, causing the node to crash, causing denial-of-service (DoS), or potentially allowing remote code execution.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS)[1] for both v3.1[2] and v4.0[3].

The indicated Common Weakness Enumerations (CWE) have been selected from the MITRE CWE list[4].

CVE-2025-15467: Stack buffer overflow in CMS (Auth)EnvelopedData parsing

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.

CVSS

CVSS v3.1 Base Score:	9.8 (critical)
CVSS v3.1 Temporal Score:	8.5 (high)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
CVSS v4.0 Score	9.3 (critical)
CVSS v4.0 Vector:	AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE

CWE-787: Out-of-bounds Write

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2025-15467

---

[1] Common Vulnerability Scoring System (CVSS), Forum of Incident Response and Security Teams, Inc., https://www.first.org/cvss/.

[2] For the CVSS v3.1 scoring only the CVSS Base Score and the Temporal Score (if information is available) are considered in this advisory. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

[3] For the CVSS v4.0 scoring only the CVSS Base Metrics and the CVSS Supplemental Metrics (if information is available) are considered in this advisory. The CVSS Environmental and Threat Metrics, which can affect the vulnerability severity, are not provided in this advisory since they reflect the potential impact of a vulnerability within the end-user organizations' computing environment and over time depending on the vulnerability exploit maturity. Therefore, end-user organizations are recommended to analyze their situation and specify the Environmental and Threat Metrics.

[4] Common Weakness Enumeration (CWE), The MITRE Corporation, https://cwe.mitre.org/.

Mitigating factors

Refer to section “General security recommendations” for further advise on how to keep your system secure.

Workarounds

No workarounds are available

Frequently asked questions

What causes the vulnerability?

Parsing CMS AuthEnvelopedData or EnvelopedData message with maliciously crafted AEAD parameters can trigger a stack buffer overflow.

What is AC500 V3?

The AC500 V3 is a scalable range of Programmable Logic Controller (PLC). It provides solutions for small, medium and high-end applications. The AC500 V3 platform offers different performance levels and is the ideal choice for high availability, extreme environments, condition monitoring, motion control or safety solutions. It offers interoperability and compatibility in hardware and software from compact PLCs up to high end and safety PLCs.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities could cause a crash, denial-of-service (DoS), or potentially remote code execution.

How could an attacker exploit the vulnerability?

Refer to section “Vulnerability severity and details“.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit the vulnerabilities. Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

When this security advisory was issued, had this vulnerability been publicly disclosed?

Yes, the vulnerabilities have been publicly disclosed.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

General security recommendations

For any installation of software-related ABB products we strongly recommend the following (non-exhaustive) list of cyber security practices:

- Isolate special purpose networks (e.g. for automation systems) and remote devices behind firewalls and separate them from any general-purpose network (e.g. office or home networks).
- Install physical controls so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.
- Never connect programming software or computers containing programing software to any network other than the network for the devices that it is intended for.
- Scan all data imported into your environment before use to detect potential malware infections.
- Minimize network exposure for all applications and endpoints to ensure that they are not accessible from the Internet unless they are designed for such exposure and the intended use requires such.
- Ensure all nodes are always up to date in terms of installed software, operating system, and firmware patches as well as anti-virus and firewall.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

References

For the vulnerability there is an advisory from OpenSSL available from the OpenSSL website:

- OpenSSL Security Advisory [27th January 2026]

Support

For additional instructions and support please contact your local ABB service organization. For contact information, see www.abb.com/contactcenters.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	2026-03-12