ABB DOC ID: 3ADR010667
REVISION: C
DATE: 2021-01-27

CYBER SECURITY ADVISORY

# AC500 V2 unauthenticated crafted packet vulnerability

## ABBVU-ABBVREP0026-3ADR010667

## 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.*

# Affected Products

All AC500 V2 products with onboard ethernet are affected by this vulnerability.

# Vulnerability ID

ABB ID: ABBVU-ABBVREP0026-3ADR010667

# Summary

ABB is aware of public reports of a vulnerability in the product versions listed above.

The vulnerability allows attackers to stop the PLC by sending an unauthenticated crafted packet over the network. After stopping (ERR LED flashing red), physical access to the PLC is required in order to restart the application.

# Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3. 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.

CVE-2020-24685:

| | |
|---|---|
| CVSS v3 Base Score: | 8.6 (High) |
| CVSS v3 Vector: | AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H |
| CVSS v3 Link: | https://www.first.org/cvss/calculator/3.0 |

# Recommended immediate actions

ABB has developed a new firmware version 2.8.5 fixing this vulnerability. This firmware version is released for the following affected PLC types:

- PM573-ETH
- PM583-ETH

When using one of these PLC types, ABB strongly recommends updating to firmware version 2.8.5, which is available for download from the ABB website either via Automation Builder 2.4.0 (download link) or as SD card image (download link).

All affected products shall be used only as described in the manual in the chapter "Cyber security in AC500 V2 products" especially regarding defense in depth and secure operation. The manual is available from our website for download (Manual for PLC Automation with AC500 V2 and Automation Builder 2.4.0).

General information about secure operation of the AC500 products is available from our white paper "Cyber Security in the AC500 PLC family".

Once the correction will be available for the remaining PLC types, ABB strongly recommends to then also update the firmware to version 2.8.5.

# Vulnerability Details

The vulnerability allows attackers to stop the PLC by sending a single unauthenticated crafted packet over the network. After stopping (ERR LED flashing red), physical access to the PLC is required in order to restart the application.

# Mitigating Factors

Although ABB provides functionality testing on the products and updates that we release, you should institute your own testing program for any product updates or other major system updates (to include but not limited to code changes, configuration file changes, third party software updates or patches, hardware exchanges, etc.) to ensure that the security measures that you have implemented have not been compromised and system functionality in your environment is as expected.

# Workarounds

ABB has currently found no workaround for this vulnerability. Therefore the PLCs shall only be used as described in the manual in the chapter “Cyber security in AC500 V2 products”.

# Frequently Asked Questions

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

Yes

## 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.

# Acknowledgements

ABB thanks the following for working with us to help protect customers:

Yossi Reuven of SCADAfence for reporting this vulnerability following coordinated disclosure.

# Support

For additional information and support please contact your local ABB service organization. For contact information, see https://new.abb.com/contact-centers.

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