CYBER SECURITY ADVISORY

AC500V2 Webserver denial of service vulnerability

ABBVU-ABBVREP0019-3ADR010645

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

The following AC500 V2 products with onboard ethernet are affected by this vulnerability:

- PM554
- PM556
- PM564
- PM566
- PM572
- PM573

Vulnerability ID

ABB ID: ABBVU-ABBVREP0019-3ADR010645

Summary

ABB is aware of a vulnerability in the products listed above. Currently there is no fix available.

The vulnerabilities can be exploited to cause the web visualization component of the PLC to stop and not respond, leading to genuine users losing remote visibility of the PLC state. If a user attempts to login to the PLC while this vulnerability is exploited, the PLC will show an error state and refuse connections to Automation Builder.

The execution of the PLC application is not affected by this vulnerability.

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-2020-24686:

CVSS v3 Base Score:	7.5 (High)
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v3 Link:	https://www.first.org/cvss/calculator/3.1

Recommended immediate actions

To prevent exploitation of this vulnerability, 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).

In case a secure operation cannot be established, and the PLC might be accessed from untrusted networks, then the web visualization shall be disabled.

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

Vulnerability Details

The affected products offer a Java applet-based Web Interface for users to build HMI-like dashboards of the PLC state. No authentication is required, where the user enables the Web Server through the Automation Builder software and specifies a hard limit (1/2 users) for concurrent connections to the Web Interface.

Two issues exist, one through sustained web requests with arbitrarily long URLs, and one through ping floods, which cause the web server to either return 400 'Bad Request' responses for all valid requests, or the Web HMI Applet failing to load on the user's browser.

For the first issue, with arbitrarily long URLs, the web interface will return a 400 Error after a number of requests are made in quick succession, or the Java Applet for the Web HMI component will fail to load. For the second issue, given a sustained number of ICMP pings in very quick succession, the Web HMI component will stop responding, requiring the PLC to be restarted for the Web Server to return.

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?

No

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:

Richard Thomas and Tom Chothia of the University of Birmingham 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.