ABB DOC ID: ABBVU-EPBP-R-5673
REVISION: -
DATE: 2018-10-24

CYBER SECURITY ADVISORY

CMS-770 Vulnerability

ABBVU-EPBP-R-5673

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 CMS-770 is available under two brands:

- ABB
- Busch-Jaeger

Busch-Jaeger Elektro GmbH is part of the ABB Group.

2CKA008100A0351	Busch-EnergyMonitor
2CCA688307R0001	CMS-770 Control Unit

Software Version: 1.7.1 (and earlier)

Vulnerability ID

ABB ID: ABBVU-EPBP-R-5673

Summary

The ABB products in scope of this vulnerability advisory will not be updated with a new firmware. Instead the customer who applies this device within an installation will receive an updated manual with additional instructions how to securely operate it.

An attacker who successfully exploited this vulnerability could cause the product to reveal the credentials allowing to take over the entire control of the product.

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.

CVSS v3 Base Score: 8.8

CVSS v3 Temporal Score: 8.8

CVSS v3 Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:U/RC:C

CVSS v3 Link: https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:U/RC:C

Recommended immediate actions

ABB has updated the manuals of the products in scope of this advisory and strongly advises customers to follow the updated installation recommendations. Customers who still want to operate the devices need to be aware of the vulnerabilities included and are requested to mitigate risks as advised in the manuals.

At the moment there are no plans of corrective measures for this specific issue in the affected products.

At the time this advisory has been published, this version of the manual was published:

https://library.e.abb.com/public/adcab406985b4510836d4b94490ad953/2CCC481007M0201_User%20Manual.pdf

Vulnerability Details

The current device firmware allows to read out the configuration file while bypassing the user authentication mechanism. The configuration file contains sensitive information that may allow an attacker to take over the entire device.

Mitigating Factors

The device shall be installed in accordance to the latest installation instructions of the technical manual.

Recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. Such practices include that process control systems are physically protected from direct access by unauthorized personnel, 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, and others that have to be evaluated case by case. Process control systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

Frequently Asked Questions

As a customer I have the urgent need to access the device and use it from anywhere. Is it possible to access the device from remote over the Internet considering the vulnerability?

Yes, if you connect to the network where the device is connected to via VPN, ensuring that this network is protected as recommended by the technical handbook (see latest update).

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could take over the entire device as the device discloses its access credentials which may be used to any reconfiguration.

What causes the vulnerability?

The vulnerability is caused by a Software/Firmware issue that allows access to a file without prior check for authorization.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could take over the entire device as the device discloses its access credentials which may be used to any reconfiguration.

How could an attacker exploit the vulnerability?

In case the attacker has direct access to the devices IP address, she/he might call the device with a specifically crafter URL.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability. 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. For more detailed information see the updated user manual and follow the installation recommendations.

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

No, ABB received information about this vulnerability through responsible disclosure

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:

- Maxim Rupp (RuppIT) for discovering this vulnerability.

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.