ABB DOC ID: 3ADR010402
REVISION: 1
DATE: 2019-06-05

CYBER SECURITY ADVISORY

Multiple Vulnerabilities in ABB CP651 HMI

ABBVU-IAMF-1902010, ABBVU-IAMF-1902011, ABBVU-IAMF-1902012

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.

This document and parts hereof must not be reproduced or copied without written permission from ABB, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Affected Products

CP651,	order code: 1SAP551100R0001, revision index B1 with BSP UN30 V1.76 and prior
CP651-WEB,	order code: 1SAP551200R0001, revision index A0 with BSP UN30 V1.76 and prior
CP661,	order code: 1SAP561100R0001, revision index B1 with BSP UN30 V1.76 and prior
CP661-WEB,	order code: 1SAP561200R0001, revision index A0 with BSP UN30 V1.76 and prior
CP665,	order code: 1SAP565100R0001, revision index B1 with BSP UN30 V1.76 and prior
CP665-WEB,	order code: 1SAP565200R0001, revision index A0 with BSP UN30 V1.76 and prior
CP676,	order code: 1SAP576100R0001, revision index B1 with BSP UN30 V1.76 and prior
CP676-WEB,	order code: 1SAP576200R0001, revision index A0 with BSP UN30 V1.76 and prior

Vulnerability ID

ABB ID:	ABBVU-IAMF-1902010	CVE ID: TBD
ABB ID:	ABBVU-IAMF-1902011	CVE ID: TBD
ABB ID:	ABBVU-IAMF-1902012	CVE ID: TBD

Summary

ABB is aware of the vulnerability in the product versions listed above based on a private vulnerability report that is reported on ABB CP620…CP635 product line.

a. ABBVU-IAMF-1902010 ABB CP651 HMI Outdated Software Components

b. ABBVU-IAMF-1902011 ABB CP651 HMI Hardcoded Credentials

c. ABBVU-IAMF-1902012 ABB CP651 HMI Absence of Signature Verification

Updates are available that resolve all internally reported vulnerabilities in the product versions listed above:

1. New version of PB610 Panel Builder 600, V2.8.0.424 which is provided via Automation Builder 2.2, SP2, available here: http://search.abb.com/library/Download.aspx?DocumentID=9AKK107492A4167&LanguageCode=de&LanguageCode=en&LanguageCode=es&LanguageCode=fr&LanguageCode=zh&DocumentPartId=&Action=Launch
2. New version of BSP (board support package) UN30 V2.31, available here: http://search.abb.com/library/Download.aspx?DocumentID=BSPCP600UN30V231&LanguageCode=en&DocumentPartId=&Action=Launch

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.

ABBVU-IAMF-1902010 ABB CP651 HMI Outdated Software Components

CVSS v3 Base Score: 5.0 (Medium) (reporter: 6.0)

CVSS v3 Temporal Score: 4.5 (Medium)

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

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

ABBVU-IAMF-1902011 ABB CP651 HMI Hardcoded Credentials

CVSS v3 Base Score: 8.8 (High)

CVSS v3 Temporal Score: 7.9 (High)

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

ABBVU-IAMF-1902012 ABB CP651 HMI Absence of Signature Verification

CVSS v3 Base Score: 8.3 (High)

CVSS v3 Temporal Score: 7.5 (High)

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

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

Recommended Immediate Actions

The problem is corrected in the following product versions:

Board Support Package BSP UN30 V2.31

Panel Builder 600 V2.8.0.424

ABB recommends that customers apply the update of the BSPs on affected CP600 control panels to that version at the earliest convenience.

Related to RemoteClient, version 2.8.0.424 there is a feature called “Force Remote Login” that blocks any access from Remote Client if password of user declared in user management.

Vulnerability Details

ABBVU-IAMF-1902010 ABB CP651 HMI Outdated Software Components

The CP651 HMI uses outdated software components that are statically linked in to the firmware files and service binaries. These components have documented vulnerabilities and should be updated and replaced. It was possible to identify severally outdated OpenSSL and ABYSS HTTP server components.

ABBVU-IAMF-1902011 ABB CP651 HMI Hardcoded Credentials

The ABB CP651 HMI component implements hidden administrative accounts that are used during the provisioning phase of the HMI interface. These credentials allow the provisioning tool “Panel Builder 600” to flash a new interface and Tags (MODBUS coils) mapping to the HMI.

ABBVU-IAMF-1902012 ABB CP651 HMI Absence of Signature Verification

The ABB CP651 HMI uses two different transmission methods to upgrade its software components:

- Utilization of USB/SD Card to flash the device
- Remote provisioning process via ABB Panel Builder 600 over FTP

For transmission, no encryption is being on the HMI software binary files. The upgrade process does compare automatically binary files with hash values included in the update package before applying the update.

Mitigating Factors

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.

More information on recommended practices can be found in the following documents:

3BSE032547, Whitepaper - Security for Industrial Automation and Control Systems (https://library.e.abb.com/public/b1f29a78bc9979d7c12577ec00177633/3BSE032547_B_en_Security_for_Industrial_Automation_and_Control_Systems.pdf)

Workarounds

If an update of the devices is not possible for the operator, a workaround is to restrict access to the devices to only trusted parties/devices.

Frequently Asked Questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could prevent legitimate access to an affected system node, remotely cause an affected system node to stop, take control of an affected system node or insert and run arbitrary code in an affected system node.

What causes the vulnerability?

The vulnerabilities are caused

- by outdated software components that are statically linked in to the firmware files and service binaries. These components have documented vulnerabilities.
- by implementing hidden administrative accounts that are used during the provisioning phase of the HMI interface.
- by transmission methods to upgrade its software components. Neither of these transmission methods implement any form of encryption or authenticity checks against the new HMI software binary files.

What is the CP651 Control Panels?

CP651 control panels are used as human machine interfaces (HMI) for the operation of automation systems.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause the affected system node to stop or become inaccessible, allow the attacker to take control of the system node or allow the attacker to insert and run arbitrary code.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

If the CP651 control panel is connected to a network, 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. If the CP651 control panel is not connected to a network, to exploit this vulnerability an attacker would need to have physical access to an affected system node.

What does the update do?

ABBVU-IAMF-1902010 ABB CP651 HMI Outdated Software Components

In WCE today CP651 use SSL just for sendmail. Sendmail does not open ports and does not expose HMI to security issues. This part of software therefor was not updated.

ABBVU-IAMF-1902011 ABB CP651 HMI Hardcoded Credentials

The update eliminates the vulnerability by replacing the hidden administrative password that is used during the provisioning phase of the HMI interface by user´s individual ones.

PB610 online-help manual highlights the necessity of using passwords for system protection. Chapter 23 “User management and passwords” deals with password settings for the HMI application while chapter 39 “System settings” deals with password settings for control panel´s BSP. Both chapters document the administrative password, which is valid as long as no user password is defined.

ABBVU-IAMF-1902012 ABB CP651 HMI Absence of Signature Verification

There is still no signature verification: Once control panel is blocked via password, just HMI administrator can do anything where anything means: format all, access to data partition and projects, update BSP / Panel Builder 600 Suite etc. So just the administrator of an HMI with access to it can really install a BSP.

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

No, ABB received information about this vulnerability through internal investigation.

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:

Xen1thLabs, A Darkmatter Company, United Arab Emirates, Abu Dhabi for providing vulnerability details and proof of concept on ABB CP635 that becomes an investigation based for this advisory.

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.