ABB DOC ID: 3ADR010466
REVISION: 1
DATE: 2019-12-05

CYBER SECURITY ADVISORY

Multiple Vulnerabilities in ABB PB610

ABBVU-RAMF-1908001, ABBVU-RAMF-1908002, ABBVU-RAMF-1908003, ABBVU-RAMF-1908004

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

PB610 Panel Builder 600, order code: 1SAP500900R0101, versions 2.8.0.424 and earlier

Vulnerability ID

ABB ID:	ABBVU-RAMF-1908001	CVE ID: CVE-2019-18994
ABB ID:	ABBVU-RAMF-1908002	CVE ID: CVE-2019-18995
ABB ID:	ABBVU-RAMF-1908003	CVE ID: CVE-2019-18996
ABB ID:	ABBVU-RAMF-1908004	CVE ID: CVE-2019-18997

Summary

ABB is aware of a private report of four vulnerabilities in the product versions listed above.

a. ABBVU-RAMF-1908001 PB610 HMIStudio crashes after launching an empty *.JPR application file

b. ABBVU-RAMF-1908002 PB610 HMISimulator does not check content-length of the HTTP request

c. ABBVU-RAMF-1908003 PB610 HMIStudio accepts malicious DLL file in an application

d. ABBVU-RAMF-1908004 PB610 HMISimulator provides interface with access to arbitrary files

An update is available that resolves all privately reported vulnerabilities in the product versions listed above:

1. New version of PB610 Panel Builder 600, V2.8.0.460 which is provided via Automation Builder 2.2, SP4, available here: http://search.abb.com/library/Download.aspx?DocumentID=9AKK106713A4481&LanguageCode=de&LanguageCode=en&LanguageCode=es&LanguageCode=fr&LanguageCode=it&LanguageCode=zh&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-RAMF-1908001 PB610 HMIStudio crashes after launching an empty *.JPR application file

CVSS v3 Base Score:	3.9 (Low)
CVSS v3 Temporal Score:	3.2 (High)
CVSS v3 Vector:	AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L/E:U/RL:O/RC:U

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

ABBVU-RAMF-1908002 PB610 HMISimulator does not check content-length of the HTTP request

CVSS v3 Base Score:	4.3 (Medium)
CVSS v3 Temporal Score:	3.8 (Low)
CVSS v3 Vector:	AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:U/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:N/I:N/A:L/E:U/RL:O/RC:C

ABBVU-RAMF-1908003 PB610 HMIStudio accepts malicious DLL file in an application

CVSS v3 Base Score: 7.1 (High)

CVSS v3 Temporal Score: 6.2 (Medium)

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

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

ABBVU-RAMF-1908004 PB610 HMISimulator provides interface with access to arbitrary files

CVSS v3 Base Score: 4.3 (Medium)

CVSS v3 Temporal Score: 3.8 (Low)

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

Recommended immediate actions

The problems are corrected in the following product versions:

PB610 Panel Builder 600 version 2.8.0.460

ABB recommends that customers apply the update of the PB610 engineering suite on their engineering PCs to that version at the earliest convenience.

ABB recommends that customers check the PB610 application directories for the presence of any DLL files. DLL files in PB610 application directories shall be removed.

Vulnerability Details

ABBVU-RAMF-1908001 PB610 HMIStudio crashes after launching an empty *.JPR application file

Due to a lack of file length check, the HMIStudio component of ABB PB610 Panel Builder 600 versions 2.8.0.424 and earlier crashes when trying to load an empty *.JPR application file. An attacker with access to the file system might be able to cause application malfunction such as denial of service.

ABBVU-RAMF-1908002 PB610 HMISimulator does not check content-length of the HTTP request

The HMISimulator component of ABB PB610 Panel Builder 600 versions 2.8.0.424 and earlier fails to validate the content-length field for HTTP requests, exposing HMISimulator to denial of service via crafted HTTP requests manipulating the content-length setting.

ABBVU-RAMF-1908003 PB610 HMIStudio accepts malicious DLL file in an application

Path settings in HMIStudio component of ABB PB610 Panel Builder 600 versions 2.8.0.424 and earlier accept DLLs outside of the program directory, potentially allowing an attacker with access to the local file system the execution of code in the application's context.

ABBVU-RAMF-1908004 PB610 HMISimulator provides interface with access to arbitrary files

The HMISimulator component of ABB PB610 Panel Builder 600 uses the readFile/writeFile interface to manipulate the work file. Path configuration in PB610 HMISimulator versions 2.8.0.424 and earlier potentially allows acces to files outside of the working directory, thus potentially supporting unauthorized file access.

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 engineering PCs is not possible for the user, a workaround is to restrict access to the engineering PCs 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 a missing pre-check of PB610 applications (*.JPR files) before loading them. So PB610 HMIStudio does not recognize a non-suitable *.JPR application file and crashes.
- by the PB610 HMISimulator, which does not check the content-length of the HTTP request. A wrong content-length could cause a crash of the process.
- by PB610 HMIStudio, which starts to search for DLL files in the PB610 application directory. A malicious DLL file which is placed in an application directory could cause malicious effects as soon as a PB610 application (*.JPR file) in the same directory is started via double-click.
- PB610 HMISimulator provides readFile/writeFile interface without limitation on the PB610 application directory, so that the user can read/write arbitrary files.

What is the PB610 Panel Builder 600?

PB610 Panel Builder 600 – HMIStudio.exe – is the engineering tool for designing HMI applications and providing the runtime for control panels, which are used for the operation of automation systems.

HMSimulator, which is made available with the installation of PB610 Panel Builder 600, is a simulation tool for efficient testing of a PB610 application in the engineering PC, before downloading it to a control panel and setting it into operation.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities 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 an engineering PC with a PB610 HMISimulator is connected to a network, an attacker who has network access to an affected system node could exploit this vulnerability. Recommended practices include that engineering PCs 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 engineering PC 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-RAMF-1908001 PB610 HMIStudio crashes after launching an empty *.JPR application file

The update eliminates the vulnerability by pre-checking a PB610 application (*.JPR file) before loading it. If the *.JPR file is no application suitable for PB610 HMIStudio, the loading is aborted with a “invalid file” message.

ABBVU-RAMF-1908002 PB610 HMISimulator does not check content-length of the HTTP request

The update includes a validation check of the content-length. A content-length less than zero returns a http error 400. A maximum value for the content-length is defined in order to avoid excess memory allocation.

ABBVU-RAMF-1908003 PB610 HMIStudio accepts malicious DLL file in an application

In the update the current/application directory is removed from the DLL search path.

ABBVU-RAMF-1908004 PB610 HMISimulator provides interface with access to arbitrary files

Access of the CGI interface ReadFile/WriteFile is limited to the PB610 application directory.

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:

NSFOCUS for providing vulnerability details and proof of concept.

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.