ABB DOC ID: 3ADR010377
REVISION: 2
DATE: 2019-06-13

CYBER SECURITY ADVISORY

Multiple Vulnerabilities in ABB PB610

ABBVU-IAMF-1902004, ABBVU-IAMF-1902005, ABBVU-IAMF-1902006, ABBVU-IAMF-1902007, ABBVU-IAMF-1902008, ABBVU-IAMF-1902009, ABBVU-IAMF-1902010

Notice

Affected Products

PB610 Panel Builder 600, order code: 1SAP500900R0101, versions 1.91 … 2.8.0.367

Vulnerability ID

ABB ID:	ABBVU-IAMF-1902004	CVE ID: CVE-2019-7225
ABB ID:	ABBVU-IAMF-1902005	CVE ID: CVE-2019-7226
ABB ID:	ABBVU-IAMF-1902006	CVE ID: CVE-2019-7227
ABB ID:	ABBVU-IAMF-1902007	CVE ID: CVE-2019-7228
ABB ID:	ABBVU-IAMF-1902008	CVE ID: CVE-2019-7230
ABB ID:	ABBVU-IAMF-1902009	CVE ID: CVE-2019-7232
ABB ID:	ABBVU-IAMF-1902010	CVE ID: CVE-2019-7231

Summary

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

a. ABBVU-IAMF-1902004 PB610 hidden administrative accounts
b. ABBVU-IAMF-1902005 PB610 IDAL HTTP Server Authentication Bypass
c. ABBVU-IAMF-1902006 PB610 IDAL FTP Server Path Traversal
d. ABBVU-IAMF-1902007 PB610 IDAL HTTP server uncontrolled format string
e. ABBVU-IAMF-1902008 PB610 IDAL FTP server uncontrolled format string
f. ABBVU-IAMF-1902009 PB610 IDAL HTTP server stack-based buffer overflow
g. ABBVU-IAMF-1902010 PB610 IDAL FTP server buffer overflow

Updates are available that resolve all privately 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) UN31 V2.31, available here: http://search.abb.com/library/Download.aspx?DocumentID=BSPCP600UN31V231&LanguageCode=en&DocumentPartId=&Action=Launch
3. 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-1902004 PB610 hidden administrative accounts

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-1902005 PB610 IDAL HTTP Server Authentication Bypass

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-1902006 PB610 IDAL FTP Server Path Traversal

CVSS v3 Base Score: 7.3 (High)

CVSS v3 Temporal Score: 6.6 (Medium)

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

ABBVU-IAMF-1902007 PB610 IDAL HTTP server uncontrolled format string

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-1902008 PB610 IDAL FTP server uncontrolled format string

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-1902009 PB610 IDAL HTTP server stack-based buffer overflow

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-1902010 PB610 IDAL FTP server buffer overflow

CVSS v3 Base Score: 6.5 (Medium)

CVSS v3 Temporal Score: 5.9 (Medium)

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

Recommended immediate actions

The problems are corrected in the following product versions:

PB610 Panel Builder 600 version 2.8.0.424

ABB recommends that customers apply the update of the PB610 applications on CP600 control panels to that version at the earliest convenience.

To prevent an unauthorized login via the Remote Client, be sure to leave the “Force Remote Login” option of the Security settings checked (default setting). If you want the Remote Client to use different user and password then set new users and passwords in the users settings.

Vulnerability Details

ABBVU-IAMF-1902004 PB610 hidden administrative accounts

The ABB CP635 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. These credentials are used over both HTTP(S) and FTP. There is no option to disable or change these undocumented credentials.

ABBVU-IAMF-1902005 PB610 IDAL HTTP Server Authentication Bypass

The IDAL HTTP server CGI interface contains a URL, which allows an unauthenticated attacker to bypass authentication and gain access to privileged functions.

ABBVU-IAMF-1902006 PB610 IDAL FTP Server Path Traversal

The IDAL FTP server fails to ensure that directory change requests do not change to locations outside of the FTP servers root directory. An authenticated attacker can simply traverse outside the server root directory by changing the directory with “cd ..”.

ABBVU-IAMF-1902007 PB610 IDAL HTTP server uncontrolled format string

The IDAL HTTP server is vulnerable to memory corruption through insecure use of user supplied format strings. An attacker can abuse this functionality to bypass authentication or execute code on the server.

ABBVU-IAMF-1902008 PB610 IDAL FTP server uncontrolled format string

The IDAL FTP server is vulnerable to memory corruption through insecure use of user supplied format strings. An attacker can abuse this functionality to bypass authentication or execute code on the server.

ABBVU-IAMF-1902009 PB610 IDAL HTTP server stack-based buffer overflow

The IDAL HTTP server is vulnerable to a stack-based buffer overflow when a large host header is sent in a HTTP request. The host header value overflows a buffer and can overwrites the Structured Exception Handler (SEH) address with a larger buffer.

ABBVU-IAMF-1902010 PB610 IDAL FTP server buffer overflow

The IDAL FTP server is vulnerable to a buffer overflow where a large string is sent by an authenticated attacker that causes a buffer overflow. This overflow is handled, but terminates the process.

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

All six of the vulnerabilities can be exploited via the network. If an update of the devices is not possible for the operator, a workaround is to restrict network 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 implementing hidden administrative accounts that are used during the provisioning phase of the HMI interface.
- by the IDAL HTTP server CGI interface containing a URL, which allows an unauthenticated attacker to bypass authentication and gain access to privileged functions.
- by the IDAL FTP server failing to ensure that directory change requests do not change to locations outside of the FTP servers root directory. An authenticated attacker can simply traverse outside the server root directory by changing the directory with “cd ..”.

- by the IDAL HTTP server being vulnerable to memory corruption through insecure use of user supplied format strings. An attacker can abuse this functionality to bypass authentication or execute code on the server.
- by the IDAL FTP server being vulnerable to memory corruption through insecure use of user supplied format strings. An attacker can abuse this functionality to bypass authentication or execute code on the server.
- by the IDAL HTTP server being vulnerable to a stack-based buffer overflow when a large host header is sent in a HTTP request. The host header value overflows a buffer and can overwrite the Structured Exception Handler (SEH) address with a larger buffer.
- By the IDAL FTP server being vulnerable to a buffer overflow where a large string sent by an authenticated attacker that causes a buffer overflow. This overflow is handled, but terminates the process.

What is the PB610 Panel Builder 600?

PB610 Panel Builder 600 is the engineering tool for designing HMI applications and the runtime for control panels, which are used 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 a control panel with a PB610 HMI application 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 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-1902004 PB610 hidden administrative accounts

The update eliminates the vulnerability by replacing the hidden administrative passwords that are 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” 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-1902005 PB610 IDAL HTTP Server Authentication Bypass

The interface 'http://localhost/cgi/loginDefaultUser' is used by Client to retrieve the default username/password in case that ForceRemote Login is disabled and the Project has a User that has been configured as DefaultUser. In the update default setting of ForceRemote Login is enabled and user is highly recommended to replace DefaultUser by individual passwords. Chapter 23 of PB610 manual / online help recommends to uncheck DefaultUser in user management. If no default users are present in the project, the CGI interface does not return any information.

ABBVU-IAMF-1902006 PB610 IDAL FTP Server Path Traversal

This is vulnerability is removed starting from PB610 Panel Builder 600 V2.0

ABBVU-IAMF-1902007 PB610 IDAL HTTP server uncontrolled format string

This is vulnerability is removed starting from PB610 Panel Builder 600 V2.0

ABBVU-IAMF-1902008 PB610 IDAL FTP server uncontrolled format string

This is vulnerability is removed starting from PB610 Panel Builder 600 V2.0

ABBVU-IAMF-1902009 PB610 IDAL HTTP server stack-based buffer overflow

This is vulnerability is removed starting from PB610 Panel Builder 600 V2.0

ABBVU-IAMF-1902010 PB610 IDAL FTP server buffer overflow

This is vulnerability is removed starting from PB610 Panel Builder 600 V2.0.1

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:

Xen1thLabs, A Darkmatter Company, United Arab Emirates, Abu Dhabi 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.