ABB Software Vulnerability Report ABBVU-IAMA-9815

ABB Portable Central Collection Unit (PCCU) v7.59 Vulnerabilities

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

ABB Portable Central Collection Unit (PCCU) v7.59 PN 2103445-070.

Vulnerability ID

ABB ID: ABBVU-IAMA-9815

Summary

ABB is aware of public reports of vulnerabilities in the product version listed above. These vulnerabilities could be exploited if an attacker: compromised the PCCU software via the methods described below.

Four bugs were opened to address the vulnerabilities reported:

1 – PCCU default installation directory has lower security than the standard MS Windows C:\Program Files installation directory.

2 – PCCU can run a non-shipped version of a DLL.

3 – PCCU stores a private key and credentials in clear text.

4 – PCCU stores device security codes in the registry in clear text

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for both CVSS v2 and 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.

Bug 1 Scores:

CVSS v2 Base Score:	Undefined
CVSS v2 Temporal Score:	Undefined
CVSS v2 Vector:	AV:ND/AC:ND/Au:ND/C:ND/I:ND/A:ND
CVSS v2 Link:	http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:ND/AC:ND/Au:ND/C:ND/I:ND/A:ND)
CVSS v3 Base Score:	8.2 (Severity Rating)
CVSS v3 Temporal Score:	7.8 (Severity Rating)
CVSS v3 Vector:	AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H/E:F/RL:W/RC:C
CVSS v3 Link:	https://www.first.org/cvss/calculator/3.0#CVSS:3.0/ AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H/E:F/RL:W/RC:C
NVD Summary Link:	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-[…]

Bug 2 Scores:

CVSS v2 Base Score:	Undefined
CVSS v2 Temporal Score:	Undefined
CVSS v2 Vector:	AV:ND/AC:ND/Au:ND/C:ND/I:ND/A:ND
CVSS v2 Link:	http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:ND/AC:ND/Au:ND/C:ND/I:ND/A:ND)
CVSS v3 Base Score:	7.5 (Severity Rating)
CVSS v3 Temporal Score:	7.3 (Severity Rating)
CVSS v3 Vector:	AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H/E:F/RL:U/RC:C
CVSS v3 Link:	https://www.first.org/cvss/calculator/3.0#CVSS:3.0/

	AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H/E:F/RL:U/RC:C
NVD Summary Link:	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-[…]

Bug 3 Scores:

CVSS v2 Base Score:	Undefined
CVSS v2 Temporal Score:	Undefined
CVSS v2 Vector:	AV:ND/AC:ND/Au:ND/C:ND/I:ND/A:ND
CVSS v2 Link:	http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:ND/AC:ND/Au:ND/C:ND/I:ND/A:ND)
CVSS v3 Base Score:	5.3 (Severity Rating)
CVSS v3 Temporal Score:	5.2 (Severity Rating)
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:U/RC:C
CVSS v3 Link:	https://www.first.org/cvss/calculator/3.0#CVSS:3.0/ AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:U/RC:C
NVD Summary Link:	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-[…]

Bug 4 Scores:

CVSS v2 Base Score:	Undefined
CVSS v2 Temporal Score:	Undefined
CVSS v2 Vector:	AV:ND/AC:ND/Au:ND/C:ND/I:ND/A:ND
CVSS v2 Link:	http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:ND/AC:ND/Au:ND/C:ND/I:ND/A:ND)
CVSS v3 Base Score:	3.6 (Severity Rating)
CVSS v3 Temporal Score:	3.3 (Severity Rating)
CVSS v3 Vector:	AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N/E:P/RL:U/RC:R
CVSS v3 Link:	https://www.first.org/cvss/calculator/3.0#CVSS:3.0/ AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N/E:P/RL:U/RC:R
NVD Summary Link:	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-[…]

Corrective Action or Resolution

ABB has investigated these vulnerabilities in order to provide adequate protection to customers.

- Bug 1 and 3 are corrected in PCCU v7.61 which is available via the ABB website.
  - Bug 1 the default installation path was changed to 'C:\Program Files\ABB Totalflow\PCCU' for the initial installation. The path selected by the user is stored in a registry key which is used as the default path in subsequent installations to provide an easy update process.
  - Bug 3, the SFTP_Key subdirectory were removed from the installation including the files, totalflowuser.ppk and UserNameAndPassword.txt, contained in that subdirectory.

Bug 2 and 4 ABB recommends that customers guard assets with appropriate security measures, to prevent malicious attacks.

ABB recommends that customers apply the update at earliest convenience.

Vulnerability Details

A vulnerability exists in the following areas in the PCCU version listed above. An attacker could exploit these vulnerabilities if left unaddressed. The details of each vulnerability are as follows:

1 – PCCU default installation directory has lower security than the standard MS Windows C:\Program Files installation directory.

2 – PCCU can run a non-shipped version of a DLL. Execution of malware can result in low to severe consequences.

3 – PCCU stores a private key and credentials in clear text. The private key is for SSH access to connected products. The SSH and SFTP services in the connected products can be disabled by the customer.

4 – PCCU stores device security codes in the registry in clear text. The security codes by themselves do not provide access to a flow computer. This information must be combined with a public IP address and protocol knowledge or access to applicable software.

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.

Workarounds

The recommended security practices mentioned above, would be the preventive measures customers should take.

Frequently asked questions

What might an attacker use the vulnerability to do?

Bug 2 - An attacker who successfully gained access to the machine, could place an altered dll into the PCCU directory that could allow the attacker to insert and run arbitrary code which could cause damage in numerous ways depending on the code executed.

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:

- Herman Groeneveld

Support

For additional information and support please contact your local ABB service organization. For contact information, see www.abb.com.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.