DOCUMENT ID: 2NGA001142
REVISION: A
DATE: 2021-10-19

CYBERSECURITY ADVISORY

Certificate verification vulnerability in Update Manager of PCM600 Engineering Tool

ABBVU-ABBVREP0050-ELDS2138

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

Product type	Products and Affected Versions
Protection and Control Engineering Tool	Update Manager Client of PCM600 version 2.7 - 2.10

Vulnerability ID

ABBID: ABBVREP0050-ELDS2138

CVE-ID: CVE-2021-22278

Summary

While validating the certificates of updated PCM600 software packages to be installed, the PCM600 Update Manager validates the common name of the certificates. This ensures that the Update Manager will only accept trusted applications. This check could be bypassed by an attacker signing applications with certificates signed by a trusted entity and containing the allowed patterns inside the common name.

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 v3.1 Base Score: 6.7 (Medium)
CVSS v3 Vector: CVSSv3.1: AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

Recommended actions

To minimize the risk of the Update Manager vulnerabilities users should take these defensive measures:

- Install latest PCM600 Update Manager version 2.4.21218.1

It is recommended to have all assets updated with the latest firmware and security patches.

Vulnerability details

The PCM600 Update manager versions listed above have a logic error that allow a user with administrator rights to install own software packages. An attacker could exploit the vulnerabilities by creating own software packages and sign those packages with specially crafted certificates and point the PCM600 update server location to an own server location.

ABB has analyzed the vulnerability.

NVD CVSS3.1 score: 6.7 (Medium)
Effect: This vulnerability may allow installation of untrusted software packages.
Mitigation: The vulnerability action should be mitigated by installing the recommended PCM600 Update Manager version 2.4.21218.1. If not, it is recommended to check the update server location to be https://toolupdate.fi.abb.com.

Frequently asked questions

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could get unwanted software packages to be installed on computer which has PCM600 installed.

What causes the vulnerability?

The vulnerability is caused by a flaw in the certificate validation of the PCM600 Update Manager.

How could an attacker exploit the vulnerability?

An attacker can sign a not officially issued software package using a certificate from a trusted root authority in which the common name matches patterns allowed in the pattern validation flaw. In addition, he has to point the update server location to an own server. Then the signed software packages can then be installed by a user with administrator access to the PCM600 workstation.

Could the vulnerability be exploited remotely?

No.

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

No

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

No

Will ABB deliver software patches for this vulnerability?

Yes, PCM600 Update Manager version 2.4.21218.1 and newer versions contain the fix for this issue.

Acknowledgement

ABB thanks CyTRICS researcher May Chaffin for helping to identify the vulnerabilities and protecting our customers.

Support

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

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

Revisions

Rev.	Page (P) Chapt. (C)	Description	Date
A	all	New document	2021-10-19