DOCUMENT ID: 2NGA002251
REVISION: A
DATE: 2024-06-25

CYBER SECURITY ADVISORY

ABB PCM600 Installer Vulnerability

CVE ID: CVE-2024-24810

ABBVREP0152

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.

Purpose

ABB has a rigorous internal cyber security continuous improvement process which involves regular testing with industry leading tools and periodic assessments to identify potential product issues. Occasionally an issue is determined to be a design or coding flaw with implications that may impact product cyber security.

When a potential product vulnerability is identified or reported, ABB immediately initiates our vulnerability handling process. This entails validating if the issue is in fact a product issue, identifying root causes, determining what related products may be impacted, developing a remediation, and notifying end users and governmental organizations.

The resulting Cyber Security Advisory intends to notify customers of the vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk as much as possible. The release of a Cyber Security Advisory should not be misconstrued as an affirmation or indication of an active threat or ongoing campaign targeting the products mentioned here. If ABB is aware of any specific threats, it will be clearly mentioned in the communication.

The publication of this Cyber Security Advisory is an example of ABB's commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information which is essential to help ensure our customers are fully informed.

Affected products

ABB protection and control IED manager PCM600.

The following PCM600 versions and Hotfix packages are affected:

ABB PCM600 version 2.11 and its Hotfixes prior to Hotfix 20240426

ABB PCM600 version 2.12 and its Hotfixes prior to Hotfix 20240520

ABB PCM600 version 2.13

Vulnerability IDs

CVE-2024-24810
ABBVREP0152

Summary

An available update resolves a publicly reported vulnerability in the product versions listed above. There is a vulnerability in the WiX toolset, which is used in packaging the PCM600 software.

An authenticated unprivileged attacker who successfully exploited this vulnerability could elevate privileges of maliciously inserted DLL files during PCM600 installation, enabling code execution with elevated privileges.

Recommended immediate actions

The problem is corrected in the following product versions:

ABB PCM600 version 2.11 base package and Hotfix 20240426

ABB PCM600 version 2.12 base package and Hotfix 20240520

ABB PCM600 version 2.13 base package

ABB recommends that customers download and apply the updates at earliest convenience. The software can be downloaded using the following link:
https://new.abb.com/medium-voltage/digital-substations/software-products/protection-and-control-ied-manager-pcm600/pcm600-downloads.

Previously stored affected PCM600 installation packages should be deleted, preventing accidental re-use.

Vulnerability severity and details

A vulnerability exists in the WiX toolset used in packaging the product versions listed above. An attacker could exploit the vulnerability by injecting libraries to the temporary folder used by the PCM600 installer, allowing the attacker to run arbitrary code with elevated privileges.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for v3.1[1].

CVE-2024-24810 Installer Vulnerability

CVSS v3.1 Base Score:	7.8
CVSS v3.1 Temporal Score:	7.0
CVSS v3.1 Vector:	AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2024-24810

Mitigating factors

The vulnerability can only be exploited during the installation phase. If acquiring the new installation packages is not possible, the administrator should take actions that no other user can log in while installing the PCM600. This will prevent other users from exploiting the vulnerability.

Refer to section “General security recommendations” for further advise on how to keep your system secure.

[1] For the CVSS v3.1 scoring only the CVSS Base Score and the Temporal Score (if information is available) are considered in this advisory. 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.

Frequently asked questions

What is the scope of the vulnerability?

The vulnerability is related to the WiX toolset, which is used in packaging the PCM600 software.

What causes the vulnerability?

There is a flaw in the WiX toolset, in the loading of the dynamic link libraries from the user's temporary directory instead of system temporary directory, when the installer is run as unprivileged user. This enables the user to insert malicious libraries into the temporary directory and have them run with administrator privileges.

What is PCM600?

The PCM600 is a tool used for engineering, analyzing, and monitoring ABB Relion® protection relays.

What might an attacker use the vulnerability to do?

An unprivileged attacker who successfully exploited this vulnerability could run arbitrary code with elevated privileges at the time, when the PCM600 installation is ongoing.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability during PCM600 installation by inserting arbitrary code into the user's temporary directory which would be run with administrator privileges. Such code could e.g., try to take control of the operating system and the configured product.

Could the vulnerability be exploited remotely?

A local, authenticated access to the PCM600 is needed as the vulnerability is not bound to the network stack. However, if there is an exploitable remote access to the PCM600, an attacker could utilize that for exploiting the PCM600 vulnerability.

Can functional safety be affected by an exploit of this vulnerability?

Yes, in case the attacker would obtain privileged access to the PCM600 host computer and subsequently to the configured product (e.g., a protection relay).

What does the update do?

The update removes the vulnerability by updating the WiX toolset.

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

Yes, the vulnerability had been publicly disclosed.

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.

General security recommendations

For any installation of software-related ABB products we strongly recommend the following (non-exhaustive) list of cyber security practices:

- Isolate special purpose networks (e.g., for automation systems) and remote devices behind firewalls and separate them from any general-purpose network (e.g., office or home networks).
- Install physical controls so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.
- Never connect programming software or computers containing programing software to any network other than the network for the devices that it is intended for.
- Scan all data imported into your environment before use to detect potential malware infections.
- Minimize network exposure for all applications and endpoints to ensure that they are not accessible from the Internet unless they are designed for such exposure and the intended use requires such.
- Ensure all nodes are always up to date in terms of installed software, operating system, and firmware patches as well as anti-virus and firewall.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

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

1MRS758440, revision G, PCM600 Cyber Security Deployment Guideline

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 cyber security program and capabilities can be found at www.abb.com/cybersecurity.

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	Jun-25-2024