DOCUMENT ID: 2NGA001518
REVISION: A
DATE: 2022-11-15

CYBER SECURITY ADVISORY

ABB PCM600
Cleartext Credentials Vulnerability

CVE ID: CVE-2022-2513

ABBVREP0086

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.

Affected product versions: PCM600 2.11 and previous versions, including hotfixes prior to 20220923.

Vulnerability IDs

CVE-2022-2513

ABBVREP0086

Summary

An available update resolves a privately reported vulnerability in the product versions listed above. There is an implementation flaw that the credentials (i.e., username and password) of IEDs are stored as clear text in the backup files.

An attacker who successfully exploited this vulnerability could obtain the IEDs' credentials. With that information, they could gain access to the IEDs, perform unauthorized modifications, or provoke a denial of service on them.

A software patch has been released to correct the problem.

Recommended immediate actions

The problem is corrected in the following product version: ABB PCM600 version 2.11 + Hotfix 20220923

ABB recommends that customers apply the update 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.

If immediate installation of hotfix is not possible, please keep the exported backup files in a secure place.

The issue can be solved for existing backups by reimporting and exporting them, after applying the hotfix.

Vulnerability severity and details

The vulnerability exists in the exported backup file included in the product versions listed above. An attacker could exploit the vulnerability by reading the user credentials from the backup file, allowing the attacker to take control of the product.

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

CVE-2022-2513

CVSS v3.1 Base Score:	7.1
CVSS v3.1 Temporal Score:	6.8
CVSS v3.1 Vector:	AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/E:X/RL:O/RC:C

NVD Summary Link:
https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=
AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/E:X/RL:O/RC:C &version=3.1

Mitigating factors

It is recommended to implement and continuously revise least privileges principles to minimize permissions and accesses to PCM600 related resources, including the PCMI/PCMP/PCMA/PCMT files.

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

Frequently asked questions

What is the scope of the vulnerability?

The backup files (PCMI, PCMP, PCMA and PCMT) produced by ABB protection and control IED manager PCM600 are including cleartext user credentials. An attacker having access to a backup file could read the user credentials and depending on which credentials are included in the backup file, would have privileged or non-privileged access to the device.

[1] 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.

What causes the vulnerability?

The vulnerability is caused by storing the cleartext user credential data in the backup files of the PCM600. When the project is exported to a backup file (PCMI, PCMP, PCMA or PCMT), the user credentials of the IED are included in the backup file in a cleartext form.

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 attacker who successfully exploited this vulnerability could obtain the user credentials of the protection relay and use them to take control of the protection relay.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by reading the user credentials from the backup file with e.g., a hex editor. If an attacker obtains the user credentials, they can be used for accessing the protection relay, performing unauthorized modifications, or provoking a denial-of-service on the protection relay.

Could the vulnerability be exploited remotely?

A local 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 have access to the affected device and the exposed password would allow privileged access for controlling the affected device.

What does the update do?

The update removes the vulnerability by not storing the cleartext passwords to the exported backup file.

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.

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 E, PCM600 Cyber Security Deployment Guideline

Acknowledgement

ABB thanks PSE - Polskie Sieci Elektroenergetyczne (Polish Power Grid Company (PPGC)) for helping to identify the vulnerability 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 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	Nov-15-2022