DOCUMENT ID: 2NGA003179
REVISION: A
DATE: 2026-09-28

CYBER SECURITY ADVISORY

ABB Protection and Control IED Manager (PCM600)
PCM600 Project Import Path Traversal
CVE ID: CVE-2026-15953

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.

© Copyright 2026 ABB. All rights reserved.

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 versions 2.14 and old.

Vulnerability IDs

CVE-2026-15953

Summary

ABB is aware of a privately reported vulnerability affecting the PCM600 project import functionality. An update is available that resolves this vulnerability in the affected product versions.

A specially crafted PCM600 project archive may exploit insufficient validation of archive entry paths during project import. Successful exploitation could allow an attacker to create or overwrite files outside the intended extraction directory using the permissions of the importing user.

Recommended immediate actions

The problem is corrected in the following product version:

ABB Protection and Control IED Manager (PCM600) version **2.14 Hotfix 20260923**.

This fixed version is available through the **ABB Update Manager** and **ABB website: PCM600 | ABB**

ABB recommends that customers upgrade to the available hotfix at the earliest opportunity. Until the update can be applied, customers should follow the mitigation measures described in this advisory.

© Copyright 2026 ABB. All rights reserved.

Vulnerability severity and details

A vulnerability exists in the PCM600 project import functionality responsible for extracting files from imported project archives. The affected implementation does not sufficiently validate archive entry paths before extracting files to disk.

A specially crafted archive may contain path traversal sequences causing files to be extracted outside the intended destination directory. Successful exploitation could allow unauthorized file creation or file overwrite operations with the privileges of the importing user.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS)[1] for both v3.1[2] and v4.0[3].

The indicated Common Weakness Enumerations (CWE) have been selected from the MITRE CWE list[4].

CVE-2026-15953 - Path Traversal During Project Archive Import

A vulnerability exists in the processing of PCM600 project archives files. Insufficient validation of archive entry paths may permit path traversal during extraction, potentially allowing files to be written to locations outside the intended extraction directory.

CVSS

CVSS v3.1 Base Score:	5.0
CVSS v3.1 Temporal Score:	4.5
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CVSS v4.0 Score	5.6
CVSS v4.0 Vector:	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:A/VC:N/VI:H/VA:N/SC:N/SI:H/SA:N

CWE

CWE - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (4.20)

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/cve-2026-15953

[1] Common Vulnerability Scoring System (CVSS), Forum of Incident Response and Security Teams, Inc., https://www.first.org/cvss/.

[2] 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.

[3] For the CVSS v4.0 scoring only the CVSS Base Metrics and the CVSS Supplemental Metrics (if information is available) are considered in this advisory. The CVSS Environmental and Threat Metrics, which can affect the vulnerability severity, are not provided in this advisory since they reflect the potential impact of a vulnerability within the end-user organizations' computing environment and over time depending on the vulnerability exploit maturity. Therefore, end-user organizations are recommended to analyze their situation and specify the Environmental and Threat Metrics.

[4] Common Weakness Enumeration (CWE), The MITRE Corporation, https://cwe.mitre.org/.

© Copyright 2026 ABB. All rights reserved.

Mitigating factors

The risk is significantly reduced when PCM600 is configured with **High Security Level**, as unsigned project files cannot be imported. As a result, attackers cannot rely on users importing manipulated unsigned archives.

Organizations that restrict project imports to trusted sources and enforce High Security Level settings substantially reduce exposure to this vulnerability.

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

Frequently asked questions

What causes the vulnerability?

The vulnerability is caused by insufficient validation of archive entry paths during extraction of imported PCM600 project archives. A specially crafted archive may exploit path traversal sequences to write files outside the intended extraction directory.

What might an attacker use the vulnerability to do?

An attacker could create or overwrite files outside the intended extraction directory using the permissions of the user who performs the import operation.

How could an attacker exploit the vulnerability?

An attacker could create a specially crafted PCM600 project archive and persuade a user to import it into PCM600. During archive extraction, traversal paths contained within the archive could result in files being written outside the intended extraction directory.

Could the vulnerability be exploited remotely?

No, the vulnerability requires user interaction. An attacker must first deliver a specially crafted project archive and convince a user to import it into PCM600.

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

The reported vulnerability affects the project archive import process on the engineering workstation. But the configuration and IED functionality will remain unaffected, even if the project backup files contains extra content that is not part of the PCM600-defined template format. However, unauthorized modification of files on an engineering workstation could potentially be leveraged for additional malicious activities depending on the deployment environment.

What does the update do?

The update removes the vulnerability by strengthening validation of archive entry paths during project import operations and preventing project archive contents from being extracted outside the intended destination directory.

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

No, ABB received information about this vulnerability through responsible disclosure.

© Copyright 2026 ABB. All rights reserved.

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.

Acknowledgement

ABB would like to thank Abhinav Agarwal for identifying this vulnerability and for reporting it in a professional manner.

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	28-09-2026

© Copyright 2026 ABB. All rights reserved.

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date

© Copyright 2026 ABB. All rights reserved.