DOCUMENT ID: 2NGA003170
REVISION: A
DATE: 2026-09-28

CYBER SECURITY ADVISORY

ABB Protection and Control IED Manager PCM600 Scheduler Service Privilege Escalation Vulnerability

CVE ID: CVE-2026-15952

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 older.

Vulnerability IDs

CVE-2026-15952

Summary

ABB is aware of a reported vulnerability in ABB Protection and Control IED Manager (PCM600).

A local authenticated user belonging to the PCM600 user group may be able to modify the configuration of a Windows service running with SYSTEM privileges. Successful exploitation could allow an attacker to execute arbitrary commands with elevated privileges on the affected workstation.

Note: This document references the ABBPCMSchedulerService_v214 component as implemented in PCM600 version 2.14. However, the described issue is not version-specific and applies equally to the corresponding component in other supported versions of PCM600.

Recommended immediate actions

ABB recommends configuring the Scheduler Service to run using the same Windows account that is used to operate PCM600, rather than using an elevated service account. Refer to the 'Workarounds' section for more information.

© Copyright 2026 ABB. All rights reserved.

Vulnerability severity and details

The vulnerability affects the PCM600 Scheduler Service (**ABBPCMSchedulerService_v214**) running under the Windows **LocalSystem** account.

The service permissions assigned during installation grant access rights to members of the local users group. This leads to privilege escalation, which could lead to compromise of the engineering workstation.

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-2026-15952 - Improper Permission Assignment in Scheduler Service

A vulnerability exists in the Scheduler Service installed with PCM600. The service executes under the LocalSystem account while permissions are granted to standard PCM600 users through membership in the local users group. An attacker with local access and valid user credentials may exploit this vulnerability to elevate privileges and obtain control of the affected host.

CVSS

CVSS v3.1 Base Score:	6.4
CVSS v3.1 Temporal Score:	5.9
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:W/RC:C
CVSS v4.0 Score	7.1
CVSS v4.0 Vector:	CVSS:4.0/AV:L/AC:H/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE

CWE - CWE-732: Incorrect Permission Assignment for Critical Resource (4.20)

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/cve-2026-15952

[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.

Workarounds

ABB recommends the following workaround. Although this workaround does not correct the underlying vulnerability, it reduces the risk of privilege escalation.

Configure the appropriate ABBPCMSchedulerService instance to run using the same Windows account that is used to operate PCM600.

- Open Services.msc.
- Locate the ABBPCMSchedulerService corresponding to the installed PCM600 version.
- Open Properties and select the Log On tab.
- The service should be configured to log on with the same Windows user account that is used for the PCM600 application.
- Ensure that this account has the required **"Log on as a service"** privilege.

When authentication is enabled for the IED, the Scheduler tool must be used with the same Windows account configured as the Scheduler Service logon account.
For installations using IED security certificates, the PCM600 setting **Always trust IED security certificates** must be enabled only when PCM600-to-IED communication takes place in a secure and trusted environment.

Impact of Workaround

- Scheduler functionality will operate using the privileges of the configured Windows user account rather than SYSTEM privileges.
- Users may need to be granted the "Log on as a service" Windows user right.
- In environments using IED security certificates, enabling Always trust IED security certificates may reduce certificate validation protections and should only be used in secure and trusted environments.
- Administrative effort may be required to maintain consistent user accounts between PCM600 and the Scheduler Service.

Frequently asked questions

What causes the vulnerability?

The vulnerability is caused by excessive permissions assigned to the PCM600 Scheduler Service. Members of the PCMSERVER2014 Users group are granted permissions allowing modification of a Windows service that executes under the LocalSystem account.

What is PCM600 Scheduler Service?

The Scheduler Service is a PCM600 system tool that runs in the background to enable task and job scheduling within PCM600. Once active, it allows users to create, configure, and manage scheduled tasks that automatically perform specified functions at designated times.

What might an attacker use the vulnerability to do?

An attacker who successfully exploits this vulnerability could execute arbitrary commands with SYSTEM privileges on the engineering workstation. This may allow the attacker to read or modify project data, alter system configuration, install software, disable security controls, and gain complete control of the affected host.

© Copyright 2026 ABB. All rights reserved.

How could an attacker exploit the vulnerability?

An attacker with local access and valid credentials could modify the configuration of the vulnerable Windows service and replace its executable path with a malicious command. When the Scheduler service is started, the command would execute with LocalSystem privileges, resulting in privilege escalation.

Could the vulnerability be exploited remotely?

No. An attacker would require local access to an affected workstation and a valid Windows account that belongs to the Local Users group. The vulnerability cannot be exploited directly over a network connection.

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

The reported vulnerability affects the Windows engineering workstation hosting PCM600. The report did not demonstrate direct impacts on connected protection relays or functional safety functions. However, a compromised engineering workstation could potentially be used as a platform for further unauthorized actions within the operational environment.

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.

© Copyright 2026 ABB. All rights reserved.

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.