DOCUMENT ID: 3BHS973333
REVISION: A
DATE: 2026-09-10

CYBER SECURITY ADVISORY

AC 800PEC, AC 800PEC ARM, AC 800PEC Tool, Control Terminal (xCT) and AC 800PEC Tool Cheetah Impacted by multiple vulnerabilities in Wibu CodeMeter

CVE ID: CVE-2026-81572, CVE-2026-81573, CVE-2026-81574, CVE-2026-81575, CVE-2026-81576

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

For CVE-2026-81572, CVE-2026-81573, CVE-2026-81574, CVE-2026-81575, CVE-2026-81576

Sl No	Product	Affected versions
1	AC 800PEC	All versions earlier than 5.4.5.2
2	AC 800PEC ARM	All versions
3	AC 800PEC Tool	All versions
4	AC 800PEC Tool Cheetah	All versions
5	Control Terminal (xCT)	All versions

Vulnerability IDs

CVE-2026-81572, CVE-2026-81573, CVE-2026-81574, CVE-2026-81575, CVE-2026-81576

Summary

An update is available that resolves a publicly reported vulnerability in the product versions listed above.

An attacker who successfully exploited these vulnerabilities could

- Allow arbitrary files to be deleted with system privileges (CVE-2026-81572),

© Copyright 2026 ABB. All rights reserved.

- Read potentially sensitive configuration data and overwrite selected values in Server.ini (CVE-2026-81573)
- Crash CodeMeter and disclose sensitive information such as process memory and stack canaries (CVE-2026-81574)
- Crash CodeMeter (CVE-2026-81575), or
- Read potentially sensitive license information (CVE-2026-81576)

Recommended immediate actions

The problem is corrected by Wibu in the following product versions:

- CodeMeter Runtime 8.41a
- CodeMeter Runtime 9.10

ABB recommends that customers apply the update at their earliest convenience and install the version compatible with their operating system. Both versions are available for download from the Wibu download site and can be updated independent of the tool installation: https://www.wibu.com/support/user/user-software.html. An updated version of CodeMeter Runtime containing the fixes will be integrated into the following tool versions:

- AC 800PEC: Version 5.4.5.2
- AC 800PEC ARM: Version 3.0.0.0 (Expected by Q1 2027)
- AC 800PEC Tool: Not planned, in classic lifecycle phase
- AC 800PEC Tool Cheetah: Version 3.0.0.0 (Expected by Q1 2027)
- Control Terminal (xCT): Not planned, in classic lifecycle phase

Vulnerability severity and details

Multiple vulnerabilities exist in the Wibu CodeMeter Runtime included in the product versions listed above. For details, please refer to the subchapters for the different CVEs.

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].

[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.

© Copyright 2026 ABB. All rights reserved.

CVE-2026-81572: Local Privilege Escalation in CodeMeter Runtime on Windows

cmu.exe --create-io --file C: creates a predictable temporary file under C:\CM-Stick. The directory and file paths are not properly checked for NTFS reparse points, such as junctions or symbolic links, before file operations are performed. A local attacker can create a junction at the temporary file that points to an arbitrary system path. Because CodeMeter Runtime runs with System privileges, this could allow arbitrary files to be deleted with System privileges and potentially enable local privilege escalation.

CVSS

CVSS v3.1 Base Score: 8.2 (high)
CVSS v3.1 Temporal Score: 8.2 (high)
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H/RC:C

CWE
CWE-284: Improper Access Control

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2026-81572

CVE-2026-81573: Improper Access Control in Local-Only Configuration Commands

If CodeMeter Runtime is configured as a server, the configuration command handler does not enforce networkorigin restrictions. Commands intended only for local or same-network clients can therefore be executed by arbitrary remote peers. An attacker can read potentially sensitive configuration data and overwrite selected values in Server.ini. This does include the hash of the credentials for the CodeMeter WebAdmin, enabling WebAdmin takeover.

CodeMeter Runtime is only affected by the vulnerabilities listed below if it is configured as a server. This is not the default. To verify the setting, check the profiling value IsNetworkServer:

- IsNetworkServer=1: configured as a server (affected).
- IsNetworkServer=0: not configured as a server.

CVSS

CVSS v3.1 Base Score: 8.6 (high)
CVSS v3.1 Temporal Score: 8.6 (high)
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L/RC:C

CWE
CWE-59: Improper Link Resolution Before File Access ('Link Following')

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2026-81573

CVE-2026-81574: Format String Vulnerability in Logger

The logger does not sanitize input strings in certain cases, allowing an attacker to inject printf-style format specifiers. This can be used to reliably crash CodeMeter and disclose sensitive information such as process memory and stack canaries. The attack works locally, for example by using cmu --set-proxy to set the proxy value, and remotely when combined with CVE-2026-81573 by setting General.ProxyServer and then triggering this vulnerability.

© Copyright 2026 ABB. All rights reserved.

CodeMeter Runtime is only affected by the vulnerabilities listed below if it is configured as a server. This is not the default. To verify the setting, check the profiling value IsNetworkServer:

- IsNetworkServer=1: configured as a server (affected).
- IsNetworkServer=0: not configured as a server.

CVSS

CVSS v3.1 Base Score: 8.2 (high)
CVSS v3.1 Temporal Score: 8.2 (high)
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H/RC:C

CWE
CWE-134: Use of Externally-Controlled Format String

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2026-81574

CVE-2026-81575: Missing Sanity Checks for Buffer Lengths

If configured as a server, CodeMeter Runtime accepts requests with opcode 0x5e, which contain the data length and the data itself. Missing bounds checking on the data length value can lead to out of bounds reads, causing a segmentation fault that ultimately crashes the CodeMeter Runtime.

CodeMeter Runtime is only affected by the vulnerabilities listed below if it is configured as a server. This is not the default. To verify the setting, check the profiling value IsNetworkServer:

- IsNetworkServer=1: configured as a server (affected).
- IsNetworkServer=0: not configured as a server.

CVSS

CVSS v3.1 Base Score: 7.5 (high)
CVSS v3.1 Temporal Score: 7.5 (high)
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/RC:C

CWE
CWE-130: Improper Handling of Length Parameter Inconsistency

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2026-81575

CVE-2026-81576: Improper Authentication of Session Handles

If configured as a server, CodeMeter Runtime issues handles per connection and relies on a cryptographically weak SID as sole authenticator. An attacker can brute-force the SID, recover another session's handle number, and read license information belonging to another handle.

CodeMeter Runtime is only affected by the vulnerabilities listed below if it is configured as a server. This is not the default. To verify the setting, check the profiling value IsNetworkServer:

- IsNetworkServer=1: configured as a server (affected).

© Copyright 2026 ABB. All rights reserved.

- IsNetworkServer=0: not configured as a server.

CVSS

CVSS v3.1 Base Score: 7.7 (high)
CVSS v3.1 Temporal Score: 7.7 (high)
CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N/RC:C

CWE
CWE-639: Authorization Bypass Through User-Controlled Key

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2026-81576

Mitigating factors

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

Workarounds

For CVE-2026-81573, CVE-2026-81574, CVE-2026-81575, and CVE-2026-81576: If you enabled the network server functionality at some point but no longer need it, disable it:

- Open the Registry Editor and navigate to *Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WIBUSYSTEMS\CodeMeter\Server\CurrentVersion*, then change the value of IsNetworkServer from 1 to 0.
- Restart CodeMeter.

Frequently asked questions

What causes the vulnerability?

Refer to section “Vulnerability severity and details”.

What is Wibu CodeMeter?

Wibu CodeMeter is a technology of Wibu-Systems providing secure protection and effective license management of software and digital content

What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities could

- allow arbitrary files to be deleted with system privileges (CVE-2026-81572),
- read potentially sensitive configuration data and overwrite selected values in Server.ini (CVE-2026-81573),

© Copyright 2026 ABB. All rights reserved.

- crash CodeMeter and disclose sensitive information such as process memory and stack canaries (CVE-2026-81574),
- crash CodeMeter (CVE-2026-81575), or
- read potentially sensitive license information (CVE-2026-81576).

How could an attacker exploit the vulnerability?

Refer to section “Vulnerability severity and details”.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability. Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

What does the update do?

The update removes the vulnerabilities in Wibu Codemeter described above.

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

Yes, this vulnerability has 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.

© Copyright 2026 ABB. All rights reserved.

References

For the following vulnerabilities advisories from Wibu are available from the Wibu website:

- Local Privilege Escalation in CodeMeter Runtime on Windows: WIBU-103081
- Vulnerabilities in CodeMeter Runtime If Configured as Server: WIBU-103401

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	2026-09-10

© Copyright 2026 ABB. All rights reserved.