

Product Security Advisory: WIBU-100193

Sharing rules



For the TLP version see: <https://www.first.org/tlp/>

Vulnerability Title

Remote Code Execution Vulnerabilities in PHP (Action Required for Self-Hosted/On-Premises Deployments; No Action Required For Hosted Instances)

Affected Products

Affected Products

CodeMeter License Portal 26.09 Branch < 26.09a
CodeMeter License Portal 25.09 < 25.09a
CodeMeter WebDepot < 24.09g
CodeMeter License Central 5.2 Branch < 5.2.2
CodeMeter License Central 5.1 Branch < 5.1.2
CodeMeter License Central 5.0 Branch < 5.0.1
CodeMeter License Central 4.x Branch
CodeMeter License Central 3.x Branch

Fixed Products

CodeMeter License Portal 26.09 Branch >= 26.09a
CodeMeter License Portal 25.09 >= 25.09a
CodeMeter WebDepot >= 24.09g
CodeMeter License Central 5.2 Branch >= 5.2.2
CodeMeter License Central 5.1 Branch >= 5.1.2
CodeMeter License Central 5.0 Branch >= 5.0.1

Vulnerability Details

Highest CVSSv3.1 Base Score	9.8
CVSSv3.1 Vector(s)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Highest Severity	Critical

Important Notice for Hosting Customers

CodeMeter License Central instances hosted by Wibu-Systems AG are managed by us, and no customer action is required.

Manual action is mainly needed for CodeMeter License Central instances hosted on-premises.

Important Notice for CodeMeter License Central Extensions

For on-premises deployments, the required update procedure depends on whether the extensions run inside the Wibu-Systems-provided VM or use a customer-managed PHP runtime outside the VM. Follow the applicable remediation instructions below. PHP 8.5 is not supported.

Vulnerabilities

RCE via OOM corruption (CVE-2026-109618)

Description

The security vulnerability CVE-2026-109618 has been disclosed in the PHP scripting language. Because both the web interface of CodeMeter License Central and the associated CodeMeter License Central Extensions (WebDepot,

Gateways, Portal, Connectors) use PHP components, unpatched systems are affected by these vulnerabilities. CodeMeter Runtime as well as WibuKey installed locally on end-user systems are not affected.

CWE: CWE-1325:Improperly Controlled Sequential Memory Allocation

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
CodeMeter License Portal 26.09 Branch < 26.09a	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
CodeMeter License Portal 25.09 < 25.09a	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
CodeMeter WebDepot < 24.09g	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
CodeMeter License Central 5.2 Branch < 5.2.2	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
CodeMeter License Central 5.1 Branch < 5.1.2	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
CodeMeter License Central 5.0 Branch < 5.0.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
CodeMeter License Central 4.x Branch	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
CodeMeter License Central 3.x Branch	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8

Fixed

- CodeMeter License Portal 26.09 Branch >= 26.09a
- CodeMeter License Portal 25.09 >= 25.09a
- CodeMeter WebDepot >= 24.09g
- CodeMeter License Central 5.2 Branch >= 5.2.2
- CodeMeter License Central 5.1 Branch >= 5.1.2
- CodeMeter License Central 5.0 Branch >= 5.0.1

Remediations

Vendor fix (2026-10-26T12:00:00.000Z)

For hosting customers: No action is required.

For products:

- CodeMeter License Central 5.2 Branch < 5.2.2
- CodeMeter License Central 5.1 Branch < 5.1.2
- CodeMeter License Central 5.0 Branch < 5.0.1

- CodeMeter License Central 4.x Branch
- CodeMeter WebDepot < 24.09g
- CodeMeter License Portal 25.09 < 25.09a
- CodeMeter License Portal 26.09 Branch < 26.09a

Restart required: **none**

For hosting customers: No action is required.

Vendor fix (2026-10-26T12:00:00.000Z)

For on-premises deployments using the Wibu-Systems-provided CodeMeter License Central VM, update CodeMeter License Central to version 5.2.2 using our container registry.

For on-premises Kubernetes deployments using the Wibu-Systems-provided Helm chart, update your deployment to use the container images for CodeMeter License Central 5.2.2 from our container registry. The operator is responsible for configuring the Helm deployment to use the fixed images and rolling out the update. Verify that all affected workloads are running the fixed images after the rollout.

In addition, we recommend applying the preventive php.ini hardening described in the 'PHP Patch Manual' available at <https://www.wibu.com/support/developer/software-downloads.html#download-273>.

For products:

- CodeMeter License Central 5.2 Branch < 5.2.2

Restart required: **system**

For on-premises deployments using the Wibu-Systems-provided CodeMeter License Central VM, update CodeMeter License Central to version 5.2.2 using our container registry.

For on-premises Kubernetes deployments using the Wibu-Systems-provided Helm chart, update your deployment to use the container images for CodeMeter License Central 5.2.2 from our container registry. The operator is responsible for configuring the Helm deployment to use the fixed images and rolling out the update. Verify that all affected workloads are running the fixed images after the rollout.

In addition, we recommend applying the preventive php.ini hardening described in the 'PHP Patch Manual' available at <https://www.wibu.com/support/developer/software-downloads.html#download-273>.

Vendor fix (2026-10-26T12:00:00.000Z)

For on-premises deployments of CodeMeter License Central 5.1 and 5.0 using the Wibu-Systems-provided CodeMeter License Central VM, apply the PHP-Patch Update Installer for your installed version. The installer is available at: <https://www.wibu.com/support/developer/software-downloads.html#download-273> Please also follow the accompanying 'PHP Patch Manual' available at the same link for mandatory post-update configuration steps.

For on-premises Kubernetes deployments of CodeMeter License Central 5.1 using the Wibu-Systems-provided Helm chart, update your deployment to use the container images for CodeMeter License Central 5.1.2 from our container registry. The operator is responsible for configuring the Helm deployment to use the fixed images and rolling out the update. Verify that all affected workloads are running the fixed images after the rollout.

For products:

- CodeMeter License Central 5.1 Branch < 5.1.2
- CodeMeter License Central 5.0 Branch < 5.0.1

<https://www.wibu.com/support/developer/software-downloads.html#download-273>

Restart required: **system**

For on-premises deployments of CodeMeter License Central 5.1 and 5.0 using the Wibu-Systems-provided CodeMeter License Central VM, apply the PHP-Patch Update Installer for your installed version. The installer is available at: <https://www.wibu.com/support/developer/software-downloads.html#download-273> Please also follow the accompanying 'PHP Patch Manual' available at the same link for mandatory post-update configuration steps.

For on-premises Kubernetes deployments of CodeMeter License Central 5.1 using the Wibu-Systems-provided Helm chart, update your deployment to use the container images for CodeMeter License Central 5.1.2 from our container registry. The operator is responsible for configuring the Helm deployment to use the fixed images and rolling out the update. Verify that all affected workloads are running the fixed images after the rollout.

Vendor fix (2026-10-26T12:00:00.000Z)

For WebDepot and License Portal running inside the Wibu-Systems-provided CodeMeter License Central VM, update each installed product to the applicable fixed version listed in this advisory. Updates are available on our website. CodeMeter License Portal is also available in our Harbor container registry.

For CodeMeter License Central Extensions running outside the Wibu-Systems-provided VM and using a customer-managed PHP runtime, update PHP to version 8.2.35 or later within the PHP 8.2 branch, or 8.4.27 or later within the PHP 8.4 branch. **PHP 8.5 is not supported.**

Test custom extensions for compatibility before updating.

For products:

- CodeMeter WebDepot < 24.09g
- CodeMeter License Portal 25.09 < 25.09a
- CodeMeter License Portal 26.09 Branch < 26.09a

Restart required: **system**

For WebDepot and License Portal running inside the Wibu-Systems-provided CodeMeter License Central VM, update each installed product to the applicable fixed version listed in this advisory. Updates are available on our website. CodeMeter License Portal is also available in our Harbor container registry.

For CodeMeter License Central Extensions running outside the Wibu-Systems-provided VM and using a customer-managed PHP runtime, update PHP to version 8.2.35 or later within the PHP 8.2 branch, or 8.4.27 or later within the PHP 8.4 branch. **PHP 8.5 is not supported.**

Test custom extensions for compatibility before updating.

Mitigation (2026-10-26T12:00:00.000Z)

For CodeMeter License Central Version 4.x, there are two options:

1. Operating system patches via paid Ubuntu Pro Support (ESM); this has been tested and approved by Wibu-Systems.
2. Alternatively: Upgrade / migration to a fixed version of CodeMeter License Central 5.0 / 5.2 (starting with version 5.1, a separate license via Sales is required).

In addition, we recommend applying the preventive php.ini hardening described in the 'PHP Patch Manual' available at <https://www.wibu.com/support/developer/software-downloads.html#download-273>.

For products:

- CodeMeter License Central 4.x Branch

Restart required: **system**

For CodeMeter License Central Version 4.x, there are two options:

1. Operating system patches via paid Ubuntu Pro Support (ESM); this has been tested and approved by Wibu-Systems.
2. Alternatively: Upgrade / migration to a fixed version of CodeMeter License Central 5.0 / 5.2 (starting with version 5.1, a separate license via Sales is required).

In addition, we recommend applying the preventive php.ini hardening described in the 'PHP Patch Manual' available at <https://www.wibu.com/support/developer/software-downloads.html#download-273>.

Workaround (2026-10-26T12:00:00.000Z)

If you cannot update, **minimize the attack surface** by operating CodeMeter License Central behind a reverse proxy with enabled client certificate. We **strongly** recommend using this protection mechanism. Please note, however, that this does not fix the problem; it only minimizes the attack surface.

For products:

- CodeMeter License Central 5.2 Branch < 5.2.2
- CodeMeter License Central 5.1 Branch < 5.1.2
- CodeMeter License Central 5.0 Branch < 5.0.1
- CodeMeter License Central 4.x Branch
- CodeMeter License Central 3.x Branch

Restart required: **system**

If you cannot update, **minimize the attack surface** by operating CodeMeter License Central behind a reverse proxy with enabled client certificate. We **strongly** recommend using this protection mechanism. Please note, however, that this does not fix the problem; it only minimizes the attack surface.

References

- Official Advisory by PHP (external) <https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w>

RCE via stale global state (CVE-2026-109619)

Description

The security vulnerability CVE-2026-109619 has been disclosed in the PHP scripting language. Because both the web interface of CodeMeter License Central and the associated CodeMeter License Central Extensions (WebDepot, Gateways, Portal, Connectors) use PHP components, unpatched systems are affected by these vulnerabilities. CodeMeter Runtime as well as WibuKey installed locally on end-user systems are not affected.

CWE: CWE-1325:Improperly Controlled Sequential Memory Allocation

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
CodeMeter License Portal 26.09 Branch < 26.09a	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	8.1
CodeMeter License Portal 25.09 < 25.09a	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	8.1

CodeMeter WebDepot < 24.09g	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	8.1
CodeMeter License Central 5.2 Branch < 5.2.2	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	8.1
CodeMeter License Central 5.1 Branch < 5.1.2	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	8.1
CodeMeter License Central 5.0 Branch < 5.0.1	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	8.1
CodeMeter License Central 4.x Branch	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	8.1
CodeMeter License Central 3.x Branch	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	8.1

Fixed

- CodeMeter License Portal 26.09 Branch >= 26.09a
- CodeMeter License Portal 25.09 >= 25.09a
- CodeMeter WebDepot >= 24.09g
- CodeMeter License Central 5.2 Branch >= 5.2.2
- CodeMeter License Central 5.1 Branch >= 5.1.2
- CodeMeter License Central 5.0 Branch >= 5.0.1

Remediations

Vendor fix (2026-10-26T12:00:00.000Z)

For hosting customers: No action is required.

For products:

- CodeMeter License Portal 26.09 Branch < 26.09a
- CodeMeter License Portal 25.09 < 25.09a
- CodeMeter WebDepot < 24.09g
- CodeMeter License Central 5.2 Branch < 5.2.2
- CodeMeter License Central 5.1 Branch < 5.1.2
- CodeMeter License Central 5.0 Branch < 5.0.1
- CodeMeter License Central 4.x Branch

Restart required: **none**

For hosting customers: No action is required.

Mitigation (2026-10-26T12:00:00.000Z)

See remaining remediations for CVE-2026-109618.

For products:

- CodeMeter License Portal 26.09 Branch < 26.09a
- CodeMeter License Portal 25.09 < 25.09a
- CodeMeter WebDepot < 24.09g
- CodeMeter License Central 5.2 Branch < 5.2.2

- CodeMeter License Central 5.1 Branch < 5.1.2
- CodeMeter License Central 5.0 Branch < 5.0.1
- CodeMeter License Central 4.x Branch

Restart required: **system**

See remaining remediations for CVE-2026-109618.

References

- Official Advisory by PHP (external) <https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp>

WIBU-SYSTEMS AG

WIBU-SYSTEMS CERT
Zimmerstrasse 5
D-76137 Karlsruhe

Namespace: <https://wibu.com>

cert@wibu.com

References

- Official Product Alerts <https://www.wibu.com/support/product-alerts.html>

Publishing Details

Publisher WIBU-SYSTEMS AG
Website <https://www.wibu.com>
Security Advisories <https://www.wibu.com/support/security-advisories.html>

Document Details

Document Name WIBU-100193
Document version 1.0.0
Initial release date 2026-10-26T12:00:00.000Z
Current release date 2026-10-26T12:00:00.000Z
Language en-US
Status final
Also referred to
Document category csaf_security_advisory

Revision history

Version	Date of the revision	Summary of the revision
1.0.0	2026-10-26T12:00:00.000Z	Initial Version

Disclaimer

The information in this document is subject to change without notice and should not be construed as a commitment by WIBU-SYSTEMS AG. All information that relates to the future (e.g. planned software versions and release dates) is provided without guarantee. WIBU-SYSTEMS AG 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 WIBU-SYSTEMS AG 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 WIBU-SYSTEMS AG 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 WIBU-SYSTEMS AG, 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.

Sharing rules

 TLP: CLEAR 

For the TLP version see: <https://www.first.org/tlp/>