WIBU CodeMeter Runtime

Important Security Information (last update: 12.08.2026)

CodeMeter Runtime - security vulnerablities

Following critical security vulnerabilities within CodeMeter Runtime has been discovered lately.

CVE-ID pending	CodeMeter Runtime configured as a network server: Under certain conditions, security vulnerabilities could occur. Only installations with the network server function enabled are affected. CVSSv3.1 base score 7.5-8.6 (high). Note: The CVE-IDs for these vulnerabilities have been requested from MITRE and had not yet been assigned at the time of this publication. Reference: WIBU-SYSTEMS Security Advisory WIBU-103401, https://www.wibu.com/en/support/security-advisories.html

Applicability to CodeMeter Runtime

The CodeMeter Runtime is used in various Vector products as a critical component for license management. The vulnerabilities described here only apply if the CodeMeter Runtime is configured as a network server, i.e. the system is used as a license server that provides licenses to other clients in the network. This is not the default configuration. Affected are CodeMeter Runtime 8.x versions below 8.41a and CodeMeter Runtime 9.x versions below 9.10 on all operating systems.

Risk analysis

Risk Category: High Risk
Justification:
According to WIBU-SYSTEMS, under certain conditions security vulnerabilities could occur if the CodeMeter Runtime is configured as a network server. Only installations with the network server function enabled are affected. Details on the individual vulnerabilities are provided in the WIBU-SYSTEMS Security Advisory WIBU-103401.
Systems with the network server function enabled accept requests from the network and are therefore exposed to attacks from the network. Systems on which the network server functionality is not enabled are not affected.
Vector products are delivered with the network server functionality of the CodeMeter Runtime disabled, which also corresponds to the default setting of the CodeMeter installer. However, if this option has been enabled to provide dedicated systems as license servers, these systems are affected by the vulnerabilities. This option is typically enabled via Vector License Client when licenses are not used locally but provided by a central license server.
Therefore, the residual risk for Vector products is assessed as High.

WIBU CodeMeter Runtime

Important Security Information (last update: 12.08.2026)

Recommended actions

The vulnerabilities are resolved in CodeMeter Runtime 8.41a and 9.10. Ensure that all systems on which the CodeMeter Runtime is configured as a network server are updated to version 8.41a or higher (for 8.x) respectively 9.10 or higher (for 9.x). If the network server functionality was enabled at some point but is no longer needed, disable it:

- CodeMeter 9.00 or newer: run cmu --disable-network-server.
- Older versions on Windows: open the Registry Editor, navigate to HKEY_LOCAL_MACHINE\SOFTWARE\WIBU-SYSTEMS\CodeMeter\Server\CurrentVersion\ and change the value IsNetworkServer from 1 to 0, then restart CodeMeter.
- Older versions on Linux/macOS: stop CodeMeter, edit /etc/wibu/CodeMeter/Server.ini and change the value IsNetworkServer from 1 to 0 in the [General] section, then start CodeMeter again.
- Alternatively, the option can be deactivated via CodeMeter WebAdmin ("Network-Server") or Vector License Client ("Share Licenses in Local Network").

Do not expose systems with enabled network server functionality to the internet and restrict network access to trusted networks protected by the customer IT.