

Security Advisory: Third-Party Component Vulnerabilities (Wibu-Systems CodeMeter)

Date: September 2, 2026

Affected Products: WIN-911 (all versions), XLReporter (version 16+)

Status: Fix Available — Action Recommended

Summary

WIN-911 and XLReporter both incorporate Wibu-Systems CodeMeter Runtime, a third-party licensing component. Wibu-Systems has disclosed five vulnerabilities in CodeMeter Runtime versions prior to 8.41a / 9.10. We are issuing this notice in accordance with our responsible disclosure practices to inform customers and provide remediation guidance.

Affected Vulnerabilities

CVE	Description	Severity
CVE-2026-81572	Improper link resolution (NTFS reparse point handling) allowing a local attacker to leverage a predictable temp file path for arbitrary file deletion with System privileges, potentially enabling local privilege escalation.	High
CVE-2026-81573	Improper access control in the server configuration command handler; remote peers can read and overwrite Server.ini values, including WebAdmin credential hashes, enabling WebAdmin takeover.	High
CVE-2026-81574	Use of externally-controlled format strings in the logger, allowing crash and disclosure of process memory/stack canaries; can be combined remotely with CVE-2026-81573.	High
CVE-2026-81575	Improper handling of a length parameter in server-mode requests (opcode 0x5e), leading to out-of-bounds reads and a crash/denial of service.	High
CVE-2026-81576	Authorization bypass via a weak, brute-forceable session identifier, allowing an attacker to recover another session's handle and read that session's license information.	High

Impact to WIN-911 and XLReporter

These vulnerabilities exist in the underlying CodeMeter Runtime component bundled with our products for license management. However, termination of the CodeMeter runtime through CVE-2026-81575 would result in our products being unable to read their license and effectively halt functionality as if the license had been violated. Your IT team may wish to consider how CodeMeter is deployed in your environment and its network exposure when conducting their risk assessment.

Remediation

Wibu-Systems has released CodeMeter Runtime **8.41a / 9.10**, which resolves all five vulnerabilities listed above. We strongly recommend that all customers:

1. Download CodeMeter Runtime version 9.10: [User Software - Wibu-Systems](#)

OR version 8.41a (for Windows Server 2012): [User Software - Wibu-Systems](#)

1. Upgrade CodeMeter Runtime as soon as practical by running the downloaded installer. This may require a reboot.

Where CodeMeter is configured in server mode, review network exposure and restrict access to trusted hosts as an interim mitigation if immediate patching isn't possible.

References

[AdvisoryWIBU-103081.pdf](#)

[AdvisoryWIBU-103401.pdf](#)