Press Release – 9 September 2026

Wibu-Systems Joins the CVE Program as a CVE Numbering Authority

- **Wibu-Systems became a CVE Numbering Authority on August 25, 2026.**
- **The company can now assign CVE IDs and publish CVE Records for vulnerabilities affecting its own products.**
- **The new role integrates standardized vulnerability identification directly into the security processes supporting CodeMeter and other Wibu-Systems technologies.**

Direct CVE ID assignment reinforces professional vulnerability management across the Wibu-Systems product portfolio

Karlsruhe, Germany – **Wibu-Systems, a global leader in software protection, licensing, and security, has partnered with the global Common Vulnerabilities and Exposures (CVE™) Program as a CVE Numbering Authority (CNA) under the ENISA Root. Effective August 25, 2026, the company can assign CVE Identifiers (CVE IDs) and publish corresponding CVE Records for vulnerabilities affecting Wibu-Systems products.**

Why CNA Status Matters for CodeMeter

The new responsibility is particularly relevant to Wibu-Systems' technological mission. Its flagship CodeMeter platform protects software and digital intellectual property against reverse engineering, piracy, unauthorized use, and tampering. It combines code encryption, integrity protection, secure key handling, access control, and license enforcement across desktop applications, cloud services, embedded devices, and industrial systems.

Because CodeMeter can become an integral part of its customers' products, operational processes, and software-based business models, the security of the technology itself demands disciplined vulnerability handling throughout its lifecycle. Clear identification,

technical assessment, remediation, and coordinated disclosure are therefore essential complements to the protective mechanisms built into the technology.

> *"CodeMeter is designed to protect software, digital assets, and the business models built around them. This makes the security of our own technology and the way we respond when a potential vulnerability is reported an essential part of the value we provide," said Alvaro Forero, Head of Product Security Incident Response Team (PSIRT) and Security Expert at Wibu-Systems. "As a CVE Numbering Authority, we can now manage CVE assignments for our products directly within our established vulnerability handling process. This gives customers, researchers, product teams, and security professionals a precise and globally recognized reference for coordinating around the same issue."*

The CVE Program provides an internationally recognized system for identifying, defining, and cataloging publicly disclosed cybersecurity vulnerabilities. A CVE ID gives each vulnerability a unique reference that can be used consistently across vendor advisories, vulnerability databases, security tools, software inventories, and customer remediation processes.

As a CNA, Wibu-Systems assumes direct responsibility for evaluating CVE eligibility within its defined scope, assigning the appropriate CVE ID, and creating and maintaining the associated CVE Record. This removes the need to request identifiers from another CNA and brings CVE assignment closer to the technical analysis conducted by the Wibu-Systems PSIRT and the responsible product teams.

From Vulnerability Report to Coordinated Disclosure

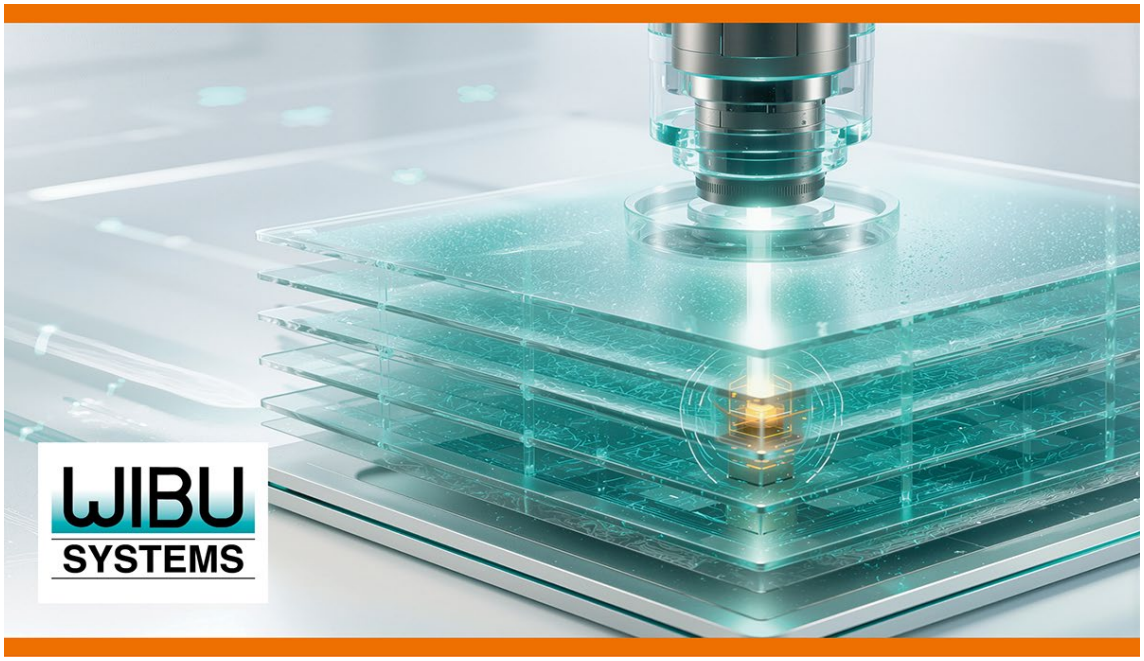
The CNA function builds on an established vulnerability management process. Wibu-Systems receives and investigates reports concerning its products, assesses their potential impact, coordinates remediation and disclosure, and publishes dedicated security advisories. Depending on the issue, these advisories can identify affected and fixed product versions, provide severity and vulnerability classifications, and describe updates, mitigations, or other recommended actions.

CVE Records and Wibu-Systems security advisories serve complementary purposes. The CVE Record provides the standardized identifier and concise vulnerability description needed by the wider cybersecurity ecosystem. The Wibu-Systems advisory supplies the product-specific technical context customers need to understand whether they are affected and what action they should take.

This combination is especially important for CodeMeter's broad deployment landscape. A vulnerability may need to be assessed differently depending on the affected component, version, license container, operating environment, attack vector, or required level of access. By connecting standardized CVE identification with detailed product advisories, Wibu-Systems can communicate these distinctions clearly without reducing a complex technical issue to an identifier or severity score alone.

Wibu-Systems operates as a CNA under the ENISA Root. The European Union Agency for Cybersecurity is the company's direct point of contact within the CVE Program and supports its alignment with the program's operational rules, processes, and defined scope.

Current Wibu-Systems security advisories and information about reporting potential vulnerabilities are available at: www.wibu.com/support/security-advisories.html



Wibu-Systems' authorization as a CVE Numbering Authority brings direct CVE assignment into the vulnerability management processes supporting CodeMeter, its technology for software protection, secure licensing, integrity protection, and digital business models.

Additional Dedicated Resources

- Press release as audio file:
  https://www.wibu.com/fileadmin/Audiofiles/press_releases/WIBU-PR_CVE_EN.mp3
- Press release images for download ready for print and online publications:
  https://wibu.sharefile.com/public/share/web-sd584d236b573430ca20b95884de74beb

About Wibu-Systems

Daniela Previtali, Global Marketing Director
Phone +49 721 9317235 / +39 035 0667070
daniela.previtali@wibu.com
https://www.wibu.com/

Wibu-Systems is a global leader in cutting-edge cybersecurity and software license lifecycle management. We are committed to delivering unparalleled, award-winning, and internationally patented security solutions that protect the intellectual property embedded in digital assets and amplify the monetization opportunities of technical know-how. Catering to software publishers and intelligent device manufacturers, the interoperable hardware and software modules of our comprehensive CodeMeter suite safeguard against piracy, reverse engineering, tampering, sabotage, and cyberattacks across mainstream platforms and diverse industries.

Media graphic resources available at: https://www.wibu.com/media-library.html.