WIBU CodeMeter WebAdmin / License Server

Important Security Information (last update: 27.05.2024)

CodeMeter WebAdmin/License Server security vulnerabilities

Following critical security vulnerabilities within CodeMeter WebAdmin / License Server has been discovered lately.

CVE-2023-24540	CodeMeter WebAdmin: GO library update required due to a critical security vulnerability.
CVE-2023-38545	CodeMeter License Server: Updated libcurl library due to a SOCKS5 protocol vulnerability.

Applicability to CodeMeter Runtime

The compromised CodeMeter Runtime is used in various Vector products as a critical component for license management. It includes CodeMeter WebAdmin and the CodeMeter License Server.

Risk analysis

The identified vulnerabilities in the CodeMeter Runtime pose significant risks to Vector products, affected products are CodeMeter Runtime <7.60d.

CVE-2023-24540:
This vulnerability in the GO library used by CodeMeter WebAdmin is extremely critical with a CVSS score of 9.8. It can potentially allow remote attackers to exploit the system via web-based interfaces, leading to unauthorized access or control over the product. This presents a high risk as it is easy to exploit and could be targeted directly through the web interface if exposed to the internet.

CVE-2023-38545:
This vulnerability in the libcurl library used by the CodeMeter License Server also has a CVSS score of 9.8. It affects the SOCKS5 protocol and could allow attackers to execute arbitrary code or conduct other malicious activities by exploiting the network communication protocol. This represents a high risk, particularly if the license server is accessible from outside the secured network.

High Risk: Both vulnerabilities are classified as high risk due to their critical nature and the potential ease of exploitation. The vulnerabilities could be exploited remotely, leading to severe consequences such as unauthorized access, system compromise, or data breaches.

Vector products that use these CodeMeter Runtime modules are consequently affected by these vulnerabilities. It is important to note that while Vector uses these modules, the vulnerabilities are inherent to the CodeMeter components provided by WIBU.

Recommended actions

The vulnerability is resolved in CodeMeter 7.60d or higher.
Ensure that the CodeMeter Runtime is updated to a version higher than CM 7.60d, which addresses these critical vulnerabilities. (The vulnerabilities are resolved in CodeMeter 7.60d or higher.)