2023-10-27
Version 1.1

# Product Security Advisory WIBU-231017-01

## Vulnerability Title

Libcurl vulnerability in CodeMeter Runtime.

## Affected products

| Product name | Affected versions | Fixed Versions |
|---|---|---|
| CodeMeter Runtime | <7.60d All platforms | >=7.60d |

## Vulnerability description

The affected Wibu-Systems' products internally use the libcurl in a version that is vulnerable to a buffer overflow attack if curl is configured to redirect traffic through a SOCKS5 proxy. A malicious proxy can exploit a bug in the implemented handshake to cause a buffer overflow. If no SOCKS5 proxy has been configured, there is no attack surface.

- CVE: CVE-2023-38545
- CVSS v3.1 base score: 9.8 (Critical)
- CVSS v3.1 vector string: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

| Product name and configuration | CVSS v3.1 environmental score | CVSS v3.1 vector string | Comments |
|---|---|---|---|
| CodeMeter Runtime not running as Network Server (default configuration) | 5.7 (Medium) | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C/MAV:L/MAC:H/MPR:H/MUI:R | Assuming that a SOCKS5 proxy is already in use or that an attacker has to set up his own SOCKS5 proxy and assuming that he has to install malware at the victim's system to manipulate the configuration of CodeMeter |
| CodeMeter Runtime running as Network Server. No SOCKS5 proxy is in use | 6.1 (Medium) | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C/MAV:A/MAC:H/MPR:L/MUI:R | Assuming that an attacker has to set up his own SOCKS5 proxy and assuming that he has to install malware at the victim's system to manipulate the configuration of CodeMeter |
| CodeMeter Runtime running as Network Server. A SOCKS5 proxy is already in use | 7.9 (High) | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C/MAV:A/MAC:L/MPR:N/MUI:N | Assuming that an attacker can use a SOCKS5 proxy that is already in use and that is correctly configured at the target |

- Vulnerability type:
  - CWE-787: Out-of-bounds Write

- Additional information:

  The attack only succeeds if the user running CodeMeter actively configured CodeMeter to use a SOCKS5 proxy – which is not the default setting. An external adversary cannot configure a proxy server for the user, so he would need to install malware to accomplish this.

  So far, we are not aware of any exploits that go beyond denial of service – which a corrupted SOCKS5 proxy could cause anyways by dropping all the messages. Yet we cannot rule out the possibility that active attacks exist that allow reading from or writing to memory that could contain secret information, or that even enable remote code execution.

**Remediation**

- Either do not use SOCKS5 proxy or update to CodeMeter Runtime >= 7.60d.

**Mitigations for affected versions**

Disable using a SOCKS5 proxy:

- The proxy environment variables HTTP_PROXY, HTTPS_PROXY **and** ALL_PROXY **must not be** set to socks5h://
- Ensure that CodeMeter is not defined to use the SOCKS5 proxy.
  The variable ProxyServer **must not be** start with socks5h://.
  - On Windows, the definition of that variable is in the registry (regedit) under HKLM/SOFTWARE/WIBU-SYSTEMS/CodeMeter/Server/CurrentVersion
  - On Mac, the definition of that variable is in the file /Library/Preferences/com.wibu.CodeMeter.Server.ini
  - On Linux, the definition of that variable is in the file /etc/wibu/CodeMeter/Server.ini
  - On Solaris, the definition of that variable is in the file /etc/opt/CodeMeter/Server.ini

**Disclaimer**

**Document History**

| Version | Date | Description |
|---|---|---|
| 1.0 | 2023-10-17 | First version without official CVSS v3.1 Base Score because it wasn't officially published yet, TLP:WHITE |
| 1.1 | 2023-10-27 | CVSS v3.1 Environmental Score calculated according to the officially published CVSS v3.1 Base Score on 25th of October 2023 |