2021-06-10
Version 1.3

Security Advisory WIBU-210423-02

Vulnerability Title

CodeMeter Runtime CmWAN Server: Denial of Service (DoS)

Vulnerability description

An attacker could send a specially crafted packet to the CodeMeter Runtime CmWAN server to cause a Denial of Service.

- CVE: CVE-2021-20094
- CVSS v3.1 base score: 7.5
- CVSS v3.1 vector string: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- Vulnerability type: CWE-126

Vulnerability details

An attacker could send a specially crafted HTTP(S) request to the CodeMeter Runtime CmWAN server that causes CodeMeter Runtime Server (i.e., CodeMeter.exe) to crash.

The recommended/standard setup is to run a CodeMeter Runtime CmWAN server only behind a reverse proxy with TLS and user authentication. If this is the case and the attacker is not on the same network as the CmWAN server, the attack is only possible for authenticated users.

If the attacker is on the same network as the CmWAN server, an unauthenticated user can perform the attack. This is only the case if the attacker can access the CmWAN port directly (default port 22351)

Affected products

Product name	Affected versions	Fixed versions
CodeMeter Runtime	All versions	7.21a

Mitigation for affected versions

- The CmWAN server is disabled by default. Please check if CmWAN is enabled and disable the feature if it is not needed.
- Run the CmWAN server only behind a reverse proxy with user authentication to prevent attacks from unauthenticated users.
- The risk of an unauthenticated attacker can be further reduced by using a host-based firewall that only allows the reverse proxy to access the CmWAN port.

General security best practices can help to protect systems from local and network attacks.

Acknowledgments

We thank Tenable, Inc. for reporting this vulnerability following coordinated disclosure.

Disclaimer

The information in this document is subject to change without notice and should not be construed as a commitment by WIBU-SYSTEMS AG. All information that relates to the future (e.g. planned software versions and release dates) is provided without guarantee.

WIBU-SYSTEMS AG provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall WIBU-SYSTEMS AG or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if WIBU-SYSTEMS AG or its suppliers have been advised of the possibility of such damages.

Document History

Version	Date	Description
1.0	2021-04-29	TLP:RED draft
1.1	2021-05-06	Integrated review feedback
1.2	2021-06-09	TLP:AMBER with restriction
1.3	2021-06-10	Final public version