Security Advisory WIBU-200521-02

Vulnerability Title
CodeMeter Runtime WebSockets API: Missing Origin Validation

Vulnerability description
This vulnerability allows an attacker to use the CodeMeter Runtime WebSockets API via a specifically crafted Java Script payload, which may allow alteration or creation of license files for CmActLicense using CmActLicense Firm Code (Firm Code 5,xxx,xxx) when combined with CVE-2020-14515.

- CVE: CVE-2020-14519
- CVSS v3.1 base score: 8.1
- Vulnerability type: CWE-346

Vulnerability details
No authentication and origin validation for WebSockets connections that allow the following actions: read licenses information, read dongle information, read CodeMeter version and update licenses.

Affected products

<table>
<thead>
<tr>
<th>Product name</th>
<th>Affected versions</th>
<th>Fixed versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CodeMeter Runtime</td>
<td>All versions prior to 7.10a</td>
<td>CodeMeter Runtime 7.10a or newer</td>
</tr>
</tbody>
</table>

Mitigation for affected versions

- The risk can be reduced by using CodeMeter Runtime 6.90 or newer. With CodeMeter Runtime 6.90 or newer no Denial of Service and no manipulation of licenses is possible, so the CVSS v3.1 base score would be reduced from 8.1 to 0.0. However the origin validation for WebSockets will be implemented in CodeMeter Runtime 7.10a.
- If it is not possible to update the CodeMeter Runtime to version 6.90 or newer then it is possible to disable the CodeMeter Runtime WebSockets API via profiling entry 'CmWebSocketApi'. In this case, the direct activation of licenses with CodeMeter License Central WebDepot will not work. However, the Software Activation Wizard using CodeMeter License Central Gateways and file-based activation in CodeMeter License Central WebDepot can still be used.

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

We thank Sharon Brizinov and Tal Keren of Claroty 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.

This document and parts hereof must not be reproduced or copied without written permission from WIBU-SYSTEMS AG, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>2020-08-14</td>
<td>Draft version</td>
</tr>
<tr>
<td>1.1</td>
<td>2020-09-07</td>
<td>Final version</td>
</tr>
</tbody>
</table>