2023-07-21
Version 1.0

Product Security Advisory WIBU-230512-01

Vulnerability Title

Vulnerability in Apache Tomcat used in Wibu-Systems' products.

Affected products

Product name	Affected versions	Fixed Versions
CodeMeter License Central	< 4.10	>= 4.10

Vulnerability description

The affected Wibu-Systems' products use the Apache Tomcat, which is vulnerable to a Request Smuggling in versions 8.5.x <8.5.83.

- CVE: CVE-2022-42252
- CVSS v3.1 base score: 7.5 (High)
- CVSS v3.1 vector string: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C

Product name	CVSS v3.1 environmental score	CVSS v3.1 vector string	Comments
CodeMeter License Central	7.2 (High)	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:L/MUI:N/MS:U/MC:N/MI:H/MA:N	The attacker needs access credentials

- Vulnerability type:
  - CWE-444 : Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
- Additional information:
  - https://lists.apache.org/thread/zzcxzvqfdqn515zfs3dxb7n8gty589sq

Remediation

- If you are using the Wibu-Systems' hosting service ("WOPS") for the affected products, then no actions are needed at your side.
- If you are not using the Wibu-Systems' hosting service ("WOPS") for the affected products, then you need to update these to the fixed versions or change configuration to "rejectIllegalHeader=true" in `/var/lib/tomee/conf/server.xml`.
  Change this:

```
<Connector port="8080"
protocol="org.apache.coyote.http11.Http11NioProtocol"
connectionTimeout="20000" redirectPort="8443" xpoweredBy="false"
server="Apache TomEE" />
```

To this configuration:

```
<Connector port="8080"
protocol="org.apache.coyote.http11.Http11NioProtocol"
connectionTimeout="20000" redirectPort="8443" xpoweredBy="false"
server="Apache TomEE" rejectIllegalHeader="true"/>
```

Mitigations for affected versions

Not required

Acknowledgments

Thanks to Sam Shahsavar who discovered this issue and reported it to the Apache Tomcat security team.

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

Version	Date	Description
1.0	2023-07-21	First public version, TLP:WHITE