2021-12-15
Version 1.1

Product Security Advisory WIBU-211213-01

Vulnerability Title

Vulnerability in Apache Log4j Library used in Wibu-Systems' products

Affected products

Product name	Affected versions	Fixed Versions
CodeMeter Keyring for TIA Portal	<=1.30 (Only the Password Manager is affected)	>1.30
CodeMeter Cloud Lite	<=2.2	>2.2

Vulnerability description

The affected Wibu-Systems' products use the Apache Log4j library, which is vulnerable to arbitrary code execution in the versions >=2.0 and <=2.14.1. From Log4j 2.15.0, the affected functionality has been disabled by default.

- CVE: CVE-2021-44228
- CVSS v3.1 base score: 10 (Critical)
- CVSS v3.1 vector string: /AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Product name	CVSS v3.1 environmental score	CVSS v3.1 vector string	Comments
CodeMeter Keyring for TIA Portal (Password Manager)	8.6 (High)	/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:W/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:H/MUI:N/MS:C/MC:H/MI:H/MA:H	The attacker needs a valid client certificate
CodeMeter Cloud Lite	9.5 (Critical)	/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:W/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:L/MPR:N/MUI:N/MS:C/MC:H/MI:H/MA:H	

- Vulnerability type:
  - CWE-400: Uncontrolled Resource Consumption
  - CWE-502: Deserialization of Untrusted Data
  - CWE-20: Improper Input Validation
- Additional information:
  - https://logging.apache.org/log4j/2.x/security.html
  - https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.html (German)

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 you can replace the Log4j library with the fixed version 2.15.0 or later.

Mitigations for affected versions

If you are not using the Wibu-Systems' hosting service ("WOPS") for the affected product(s) please consider following measures to reduce the risk until the fixed version of the affected product can be installed. Please be aware that not all mitigations apply to every possible product configuration, so please check which of these could be relevant or applicable in your case.

Implement one of the mitigation techniques below:

- Java 8 (or later) users should upgrade to release 2.16.0.
- Users requiring Java 7 should upgrade to release 2.12.2 when it becomes available (work in progress, expected to be available soon).
- Otherwise, remove the JndiLookup class from the classpath: zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class

Source of these mitigations: https://logging.apache.org/log4j/2.x/security.html

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

Acknowledgments

This issue was discovered in the log4j library by Chen Zhaojun of Alibaba Cloud 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	2021-12-14	First version, TLP:WHITE
1.1	2021-12-15	Modification of the mitigations published by Apache