2021-12-21
Version 1.0

Product Security Advisory WIBU-211220-01

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)	>=1.30a
CodeMeter Cloud Lite	<=2.2b	>=2.2c

Vulnerability description

The affected Wibu-Systems' products use the Apache Log4j library, which is vulnerable to Denial of Service in versions >=2.0-alpha1 and <=2.16.0 (excluding 2.12.3). This vulnerability is fixed in Log4j 2.17.0 (Java 8 and later), 2.12.3 (Java 7) and 2.3.1 (Java 6).

- CVE: CVE-2021-45105
- 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:N/A:H

Product name	CVSS v3.1 environmental score	CVSS v3.1 vector string	Comments
CodeMeter Keyring for TIA Portal (Password Manager)	6.4 (Medium)	/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:W/RC:C/CR:H/IR:H/AR:H/MPR:H	The attacker needs a valid client certificate
CodeMeter Cloud Lite	8.6 (High)	/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C/CR:H/IR:H/AR:H	

- Vulnerability type:
  - CWE-674: Uncontrolled Recursion
  - CWE-20: Improper Input Validation
- Additional information:
  - https://logging.apache.org/log4j/2.x/security.html
  - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45105

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 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.

This vulnerability can be mitigated in configuration:

- In PatternLayout in the logging configuration, replace Context Lookups like ${ctx:loginId} or $${ctx:loginId} with Thread Context Map patterns (%X, %mdc, or %MDC).
- Otherwise, in the configuration, remove references to Context Lookups like ${ctx:loginId} or $${ctx:loginId} where they originate from sources external to the application such as HTTP headers or user input.

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

Independently discovered in Log4j by Hideki Okamoto of Akamai Technologies, Guy Lederfein of Trend Micro Research working with Trend Micro's Zero Day Initiative, and another anonymous vulnerability researcher.

Disclaimer

Document History

Version	Date	Description
1.0	2021-12-21	First version, TLP:WHITE