LOG4J - CVE-2021-4104

PUBLISHED: JANUARY 07, 2022 | LAST UPDATE: JANUARY 07, 2022

SUMMARY

In December 2021, Apache Log4j (logging.apache.org) [1] published security advisories detailing several critical security issues. During the continued investigation it was discovered that Log4j 1.2 was vulnerable to a related issue involving JNDI and JMSAppender. This vulnerability requires JMSAppender to be enabled for a system to be exposed.

For more information on related Log4j issues affecting log4j 2.x see the A10 Networks Security Advisory titled "LOG4J - CVE-2021-44228, CVE-2021-45046, CVE-2021-45105".

The following vulnerabilities reported by Apache Log4j are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2021-4104	CVSS 3.0	8.1 High	log4j: Remote code execution in Log4j 1.x when application is configured to use JMSAppender[2]

AFFECTED PRODUCTS AND RELEASES

The table below indicates the vulnerability status of A10 products for these vulnerabilities. Unless specific models or product software releases are indicated, the vulnerability status should be considered to reflect all product models and software releases.

Product	Vulnerability Status
A10 Thunder	Not affected
A10 vThunder (Virtual Thunder)	Not affected
A10 cThunder (Container Thunder)	Not affected
A10 AX Series	Not affected
A10 aGalaxy TPS	Not affected
A10 aGalaxy ADC Series	Not affected
A10 Harmony Controller	Not affected
A10 Enterprise License Manager (ELM)	Not affected

WORKAROUNDS AND MITIGATIONS

None

SOFTWARE UPDATES

Not available

VULNERABILITY DETAILS

The following table shares brief descriptions for the vulnerabilities addressed in this document.

Vulnerability ID	Description
CVE-2021-4104	JMSAppender in Log4j 1.2 is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration. The attacker can provide TopicBindingName and TopicConnectionFactoryBindingName configurations causing JMSAppender to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-44228. Note this issue only affects Log4j 1.2 when specifically configured to use JMSAppender, which is not the default. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.

RELATED LINKS

Ref #	General Link
[1]	Apache Log4j Security Vulnerabilities
[2]	NIST NVD CVE-2021-4104

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2022-01-07	Initial Publication