IDIS

One Solution. One Company.

SN-11

Log4j Vulnerabilities

Version 1.0.1

1 Overview

This document offers a concise overview of the recently issued Apache Log4j vulnerabilities and their impact on IDIS products.

2 What are the Log4j vulnerabilities?

Almost all software will have some form of logging capability for development, operational, and security purposes. Apache Log4j is a popular open-source logging framework (APIs) written in Java, generally used by developers to monitor activities in their software applications or online services [1].

Recently, several security vulnerabilities were discovered in Log4j, enabling unauthorized users to breach systems, steal passwords and logins, extract data, and infect networks with malicious software by exploiting these weaknesses [2].

Please refer to the following reports on the CVE site for further information."

(1) CVE-2021-44228 vulnerability

> "*Apache Log4j2 2.0-beta9 through 2.12.1 and 2.13.0 through 2.15.0 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0, this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects* [3]".

(2) CVE-2021-45046 vulnerability

> "*It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in a denial of service (DOS) attack. Log4j 2.15.0 makes a best-effort attempt to restrict JNDI LDAP lookups to localhost by default. Log4j 2.16.0 fixes this issue by removing support for message lookup patterns and disabling JNDI functionality by default* [4]".

(3) CVE-2021-4104 vulnerability

> "*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 TopicConnection-FactoryBindingName 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* [5]".

3 Impacts of Log4j vulnerabilities on IDIS Products

All IDIS products and online sites are not affected by these reported vulnerabilities because Apache Log4j2 and related libraries have not been used in IDIS products.

- DirectIP NVRs (DR series) : not affected
- DirectIP Cameras (DC series) : not affected
- DirectCX TVRs (TR series) : not affected
- PC based NVRs (ID & IR series) : not affected
- ISS (IDIS Solution Suite) and ISS License Server (license.idisglobal.com) : not affected
- IDIS Center, IWS (IDIS Wall Station) : not affected
- FEN (For Every Network, fen.idisglobal.com) : not affected
- IDIS Web (local & web.idisglobal.com) : not affected
- ICM (IDIS Cloud Manager, icm.idisglobal.com) : not affected
- Push (push.idisglobal.com) : not affected
- Other client software such as IDIS Discovery, IDIS Mobile apps : not affected
- Network accessories such as network switch, storage, video encoder/decoder, etc. : not affected

- IDIS homepage (www.idisglobal.com) : not affected
- IDIS partner site (partner.idisglobal.com) : not affected
- IDIS VTS forum (forum.idisglobal.com) : not affected

Contact Us

Additional information may be updated in this document in the future. For any questions or concerns related to this issue, please email security@idisglobal.com.

References

[1] https://logging.apache.org/log4j/2.x/security.html

[2] https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228

[4] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046

[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4104

Version History

Version	Writer	Revision Date	Remarks
1.0.1	Daniel Lee	Dec. 17. 2021	Push server information has been added. Online site are not affected by these vulnerabilities.
1.0.0	Daniel Lee	Dec. 16. 2021	Initial Release