CLS-202112-B1: Log4Shell Vulnerability CVE-2021-44228 / CVE-2021-45046 in Log4J2 Open-Source Library

Publication Date: 2021-12-14

Last Update: 2021-12-15

Current Version: 1.0

CVSS v3.1 Base Score: 10.0 CRITICAL / 3.7 LOW

SUMMARY

Log4j2 is an open-source library originally from the Apache Software Foundation project and used almost ubiquitously in enterprise software products and cloud services.

On 2021-12-09, a vulnerability in Apache Log4j, a logging tool used in many Java-based applications, was disclosed, allowing remote unauthenticated attackers to execute code on vulnerable systems.

The vulnerability has been recorded as **CVE-2021-44228** and has been rated with a CVSS 3.1 score of **10.0 CRITICAL**. **CVE-2021-45046** has also been created to identify some incomplete non-default configurations with the CVE-2021-44228 fixes with a CVSS 3.1 score of **3.7 LOW**.

The following three (3) conditions need to be in place to exploit the vulnerability:

1. An application uses the vulnerable library: Log4J2 (version < 2.15RC2).
2. An attacker can inject a special command into the application via the network.
3. Outgoing requests to LDAP (Lightweight Directory Authentication Protocol) or other JNDI endpoints are not blocked.

AFFECTED PRODUCTS AND SYSTEMS

Affected Product and Versions	Remediation
Trellix 8.1.0 and earlier versions	Mitigation for immediate remediation: Configure your firewall to block outgoing LDAP packets or other JNDI endpoints from Trellix Upgrade Trellix to 8.1.2 (estimated to be released in Jan 2022) Refer to Workaround and Mitigation section for more detailed information.

WORKAROUND AND MITIGATIONS

Cooper Lighting has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Configure outbound firewall rules from the Trellix to block any LDAP packets or other JNDI endpoints.

- Cooper Lighting Solutions is working on a software update to address this vulnerability. The software update, 8.1.2, will be posted on our Support and Services portal (trellix.cooperlighting.com) as soon as it is made available. Customers who have registered to our Support and Services portal that have agreed to receive email notifications will get an email notification once the new firmware is uploaded on the portal.
  Please note that customers with Trellix 7.X and older will require to upgrade their full system prior to upgrading their Trellix Core to 8.1.2. We recommend the upgrade to be done by a certified WaveLinx specialist.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring

CVE-2021-44228:

Base Score: 10.0 CRITICAL
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVE-2021-45046:

Base Score: 3.7 LOW
Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L

REFERENCES

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

https://nvd.nist.gov/vuln/detail/CVE-2021-44228

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

https://nvd.nist.gov/vuln/detail/CVE-2021-45046

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

TERMS OF USE

Signify Security Advisories are subject to the terms and conditions contained in Signify underlying license terms or other applicable agreements previously agreed to with Signify (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Signify Security Advisory, the Terms of Use of Signify Global Website: https://www.signify.com/global/conditions-of-commercial-sale . In case of conflicts, the License Terms shall prevail over the Terms of Use.