PHILIPS
dynalite
Security Advisory

Security Advisory No. 002

Date: 22nd Dec 2021

Log4Shell Vulnerability CVE-2021-44228, CVE-2021-45046 and CVE-2021-45105 in Log4J2 Open-Source Library

Advisory ID: PD-2021-0002
Document Version: 1.1
First published: 2021-12-22
Last updated: 2022-01-11

Advisory Title

Log4Shell Vulnerability CVE-2021-44228, CVE-2021-45046 and CVE-2021-45105 in Log4J2 Open-Source Library

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.

The vulnerability has been recorded as CVE-2021-44228 has been rated with a CVSS 3.1 score of 10.0 CRITICAL.

Additionally, 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.

On December 18, a new vulnerability was disclosed that allows potentially a Denial-Of-Service Attack. This vulnerability is identified by CVE-2021-45105.

The following 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 is able to 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

Product	Affected Version	Remediation
PDDEG-S	Firmware version 1.12 and earlier	Upgrade to version 1.13, to be released shortly

Details

PDDEG-S versions 1.12 and earlier use the Log4j2 library to process internally created logging

messages. Due to the particular use of the library in the product we are not currently aware of a working exploit. As a precaution we will release new firmware that does not contain Log4j.

Obtaining Software Fixes

Software fixes will be made available through the Philips Dynalite Distributor Support website.

https://www.dynalite.org/support

General Security Recommendations

Customers using the affected devices are strongly recommended to operate the devices in closed networks or protected with a suitable firewall. Use network segmentation to minimize exposure to untrusted networks.

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.

CVSS 3.x Severity and Metrics:

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

CVE-2021-45105
Base Score: 7.5 HIGH
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

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.