interact

IA-2021-01: Log4Shell Vulnerability CVE-2021-44228 and CVE-2021-45046 and CVE-2021-45105 in Log4J2 Open-Source Library

Publication Date: 16/12/2021

Last Update: 21/12/2021

Current Version: 1.2

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 < 2.17.0);
2. An attacker is able to manipulate logs of the application to inject a command;
3. Outgoing requests to LDAP (Lightweight Directory Authentication Protocol) or other JNDI endpoints are not blocked or whitelisted.

Affected Products and Systems

The following Systems and products are affected:

Affected Product	Remediation
Interact Office POE – Envision Manager (also known as Interact Office Wired) version 1.9R2 **Version 1.8.1 and earlier do not make use of the log4j2 library and are not impacted**	Temporary mitigation: configure your firewall to block outgoing LDAP packets or other JNDI endpoints Apply a patch: A new version of pax-logging library that is not vulnerable will be made available. Please contact your customer satisfaction team for support Upgrade to version 1.9GA which will be released shortly.

Interact Landmark GW version FW < 2019.08.54.323	Upgrade to next available version which will be released shortly and is published on https://www.colorkinetics.com/global/support/downloads/firmware This new FW uses version 2.17.0 of log4j library which fixes the vulnerability

Details

Interact Office POE Envision Manager: A 3rd party library, version 1.10.2 of Pax Logging can be deployed on the Envision Manager machines, which is affected by the Log4j2 vulnerability.

Interact Landmark Gateway uses log4j2 library. If installed according to the Installation guide and product Security Statement, the gateway user interface is only accessible from the local area network.

Workaround and Mitigations

For products that support it, a mitigation which partially help reduce the exploitability of the application is to Adapt the application server start-up by adding -Dlog4j2.formatMsgNoLookups=true somewhere after the standalone.sh statement.

Block all ports for the product going out to hosts that are not whitelisted.

General Security Recommendations

Please follow the general security recommendations in the Installation Guide and the Product Security Statement provided.

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

Acknowledgements

Additional Information

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.