2022 年 2 月 8 日

お客様各位

株式会社 日立ソリューションズ
Juniper Networks 製品ユーザサポート

Apache Log4j の脆弱性(CVE-2021-44228)の Juniper 製品への影響について(最終報)

拝啓、平素は Juniper 製品サポートをご利用くださいまして誠にありがとうございます。
先日、Apache の Java ベースのログ出力ライブラリである「Apache Log4j」について、脆弱性情報(CVE-2021-44228)が公開されています。当該脆弱性に関する Juniper 製品への影響を下記にご案内します。

敬具

記

1. CVE-2021-44228 の Juniper 製品への影響

当社で取り扱っている Juniper 製品について CVE-2021-44228 の影響の有無を下記に記載します。
本件の詳細、回避策等については、Juniper Networks 社から発表されている JSA11259 (*1)をご覧ください。(関連する脆弱性 CVE-2021-4104, CVE-2021-45046, CVE-2021-42550 に関する記事が追記されました)
尚、同サイト記載内容以上の情報は開示されていません。記載内容の解釈また記載内容以上の情報については、当社サポートではお答えいたしかねます。予めご了承ください。

非該当製品（CVE-2021-44228, CVE-2021-4104, CVE-2021-45046, CVE-2021-42550 全て非該当）

- JunosOS 製品（SRX [vSRX 含む]/ EX / QFX / MX）
- ScreenOS 製品（SSG / ISG / NS5000）
- Security Director
- Security Director Insights
- Log Collector ~~20.1~~ (Log Collector は 20.1 より前のバージョンも非該当です)
- Sky Enterprise
- JATP Cloud (旧 SkyATP)

該当製品（CVE-2021-44228 に該当）

- Junos Space Network Management Platform (以下 Junos Space と略します)

※ Junos Space において OpenNMS 機能が有効な場合に本脆弱性の影響を受ける可能性がございます。(OpenNMS 機能はデフォルト有効です)

※ 保守契約ユーザ様向けに、当社サポートサイトの Junos Space ページ内に対策版のご案内、および、回避策適用に関する技術情報を掲載しています。
Junos Space をご使用のお客様は、合わせてご参照ください。(ログインが必要)

2. IPS シグネチャでの対応状況

SRX シリーズで使用可能な IPS 機能にて、本脆弱性に対応した IPS シグネチャ(HTTP:APACHE:LOG4J-JNDI-MGNR-RCE) が、シグネチャパッケージ version 3444 でリリースされています。また、version 3446 にて定義内容の更新および関連シグネチャの追加が行われています。(別紙参照)
更に、version 3448 にて、本脆弱性に対応した IPS シグネチャの定義内容が更新されました。
加えて、version 3449 にて、本脆弱性に対応した IPS シグネチャの定義内容更新、および、CVE-2021-45105 に対応したシグネチャが追加(version 3451 にて定義内容更新)されました。
また、version 3452 にて、CVE-2021-44832 に対応したシグネチャが追加されました。
シグネチャパッケージ version 3452 以降のシグネチャを SRX にインストールし、ポリシに適用することで、検知/防御が可能となります。(シグネチャは、より最新のものをご使用ください)

以上

(*1) Multiple Products: Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints. (CVE-2021-44228, CVE-2021-4104, CVE-2021-45046 and CVE-2021-42550)
https://kb.juniper.net/JSA11259

[別紙] シグネチャの属性とアタックグループについて

SRX シリーズの IPS 機能による検知/防御において、CVE-2021-44228 の脆弱性を検知するシグネチャを単体でポリシ適用する以外に、アタックグループ単位での適用も可能です。

本脆弱性対応にて追加された、シグネチャの属性は下記のとおりです。
(下記属性情報は、シグネチャパッケージ version 3461 時点の情報となります。
今後のシグネチャパッケージのリリースに伴い、属性が変更となる可能性がございます。)

ID	シグネチャ名	Severity	Category	Recommended 属性	Recommended-Action	Performance	Direction
23665	HTTP:APACHE:LOG4J-JNDI-MGNR-RCE	Critical	HTTP	TRUE	Drop	0	CTS
23666	DNS:APACHE-LOG4J-JNDI-RCE	Critical	DNS	TRUE	Drop	0	CTS
23667	APP:MISC:APACHE-LOG4J-UDPVR-RCE	Critical	APP	TRUE	Drop	0	CTS
23668	APP:MISC:APACHE-LOG4J-TCPVR-RCE	Critical	APP	TRUE	Drop	0	CTS
23671	HTTP:DOS:APACHE-LOG4J-DOS	Minor	HTTP	TRUE	Drop	0	CTS
23677	HTTP:APACHE:LOG4J-JDBC-APNDR-CE	Major	HTTP	TRUE	Drop	0	CTS

既に IPS 機能を使用されている場合、既存で設定されているアタックグループによっては、シグネチャパッケージを最新のものに更新するのみで、設定変更を行うことなく、攻撃の検知/防御が可能となっている場合もございます。

下記のコマンドにて、ご使用の SRX において対象のシグネチャが適用されているかどうかを確認可能です。
例:
> show security idp attack attack-list policy <idp-policy 名> | match log4j
※　適用されているシグネチャリストの一覧からシグネチャ名に「log4j」文字列を含む結果を出力します。

【参考】

1. ID:23665 のシグネチャは、シグネチャパッケージ version 3444 にて追加されましたが、その後、シグネチャパッケージ version 3446 にてシグネチャ内の定義が更新され、「Performance」属性が「0」から「9」に変更されました。更に、version 3448 にてシグネチャ内の定義が更新され、加えて「Performance」属性は「0」に変更されました。
   更に、version 3449 にてシグネチャ内の定義が更新され、CVE-2021-44228 に加え、CVE-2021-45046 にも対応するようになりました。

2. ID:23666、ID:23667、ID:23668 のシグネチャは、シグネチャパッケージ version 3446 にて追加されました。また、version 3448 にて定義内容が更新されました。ID:23667、ID:23668 については、「Performance」属性が「9」から「0」に変更されました。
   更に、version 3449 にてシグネチャ内の定義が更新されています。

3. ID:23671 のシグネチャは、シグネチャパッケージ version 3449 にて追加されました。
   本シグネチャは「Apache Log4j」に関する脆弱性のうち CVE-2021-45105 に対応するシグネチャです。
   なお、version 3451 にて定義内容が更新されています。

4. ID:23677 のシグネチャは、シグネチャパッケージ version 3452 にて追加されました。
   本シグネチャは「Apache Log4j」に関する脆弱性のうち CVE-2021-44832 に対応するシグネチャです。

5. 「Recommended 属性」は全て **TRUE** となっています。
   "Recommended Attacks" のアタックグループを適用している場合、シグネチャパッケージ version 3452 以降に更新することで、上記全てのシグネチャは検知/防御の対象となります。

6. 「Recommended-Action」は全て **Drop** となっています。
   ポリシ(idp-policy)におけるアクションとして「**recommended**」を指定している場合、攻撃検知と共に、パケットを破棄します。

7. 「Performance」項目は「0」「１」「５」「9」の値をとり、数字が大きいほど処理負荷が高いことを意味します。なお、SRX シリーズのシグネチャ定義においては、「0」「9」のいずれかが定義されます。
また、「Performance」項目が「9」のシグネチャは、MISC アタックグループに分類されます。

8. 「Direction」項目の「CTS」は Client to Server の略ですが、通信の開始元から宛先方向へのパケットを検査することを意味します。

9. ID:23665 のシグネチャは、シグネチャパッケージ version 3446 では、「Performance」属性が「9」であったため、"Misc_HTTP - All"、"Misc_HTTP - Critical" 等のアタックグループに分類されていましたが、シグネチャパッケージ version 3448 にて、「Performance」属性が「0」に変更されたため、"HTTP - All"、"HTTP - Critical" 等の一般的によく使用されるアタックグループを適用している環境において、ID:23665 のシグネチャが適用されるようになりました。

[改訂履歴]

改訂番号	発行年月	変更内容
初版	2021 年 12 月 14 日	新規発行
第 2 報	2021 年 12 月 17 日	1. CVE-2021-44228 の Juniper 製品への影響 • CVE-2021-4104, CVE-2021-45046 に関する記述追記 • 非該当製品の JunosOS 製品に[vSRX 含む]の補足を追記 • 非該当製品の Log Collector バージョン表記削除 • 該当製品の Junos Space の回避策適用に関する案内追記 2. IPS シグネチャでの対応状況 • シグネチャパッケージ version 3446 に関する情報追記 [別紙] • CVE-2021-44228 に対応した IPS 機能のシグネチャ詳細情報を追記
第 3 報	2021 年 12 月 21 日	1. CVE-2021-44228 の Juniper 製品への影響 • CVE-2021-42550 に関する記述追記 2. IPS シグネチャでの対応状況 • シグネチャパッケージ version 3448 に関する情報追記 [別紙] • シグネチャパッケージ version 3448 の更新に伴い説明内容を改訂
第 4 報	2021 年 12 月 24 日	2. IPS シグネチャでの対応状況 • シグネチャパッケージ version 3449 に関する情報追記 [別紙] • シグネチャパッケージ version 3449 の更新に伴う説明追記 • シグネチャパッケージ version 3449 にて追加されたシグネチャに関する情報追記
最終報 (第 5 報)	2022 年 2 月 8 日	1. CVE-2021-44228 の Juniper 製品への影響 • 該当製品の Junos Space において、脆弱性の影響を受ける可能性のある使用条件を追記 • 該当製品の Junos Space における、対策版の案内を追記 2. IPS シグネチャでの対応状況 • シグネチャパッケージ version 3452 に関する情報追記 [別紙] • シグネチャパッケージ version 3452 の更新に伴う説明追記 • シグネチャパッケージ version 3452 にて追加されたシグネチャに関する情報追記