2021 年 12 月 23 日

お客様各位

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

Apache Log4j の脆弱性(CVE-2021-44228, CVE-2021-45046, CVE-2021-45105)の Palo Alto Networks 製品への影響について（第６報）

平素は Palo Alto Networks 製品サポートをご利用下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, **CVE-2021-45046, CVE-2021-45105**）が公開されています。当該脆弱性に関する Palo Alto Networks 製品への影響を下記にご案内いたします。

※太字箇所は追記もしくは更新箇所となっています。

記

1. Palo Alto Networks 製品への影響

   CVE-2021-44228, **2021-45046 に関して、**当社で保守サービスをご提供している Panorama（M シリーズおよび Panorama VM）に影響がございます。**CVE-2021-45105 は Panorama を含め、**影響を受けません。

   ※2021/12/18 と 12/21 に関連する CVE として CVE-2021-45046 と CVE-2021-45105 が追加されました。影響範囲など一部の情報は公開されているものの、調査自体は継続中になっております。今後のアップデートによっては内容が変更される可能性がございます。

   表 1.1 影響がある Panorama の OS バージョンと稼働モード

	影響を受ける	影響を受けない
OS バージョン	9.0.*, 9.1.*, 10.0.*	8.1.*, 10.1.*
稼働モード	Panorama モード Log Collector モード	Management Only モード Legacy モード

   ・Panorama の稼働モードは以下からご確認ください。

   WebUI：Dashboard ＞ 一般的な情報 システムモード

   CLI ：＞ show system info | match system-mode

2. 回避策

   現在、メーカから公開されている、Panorama の本脆弱性に対しての回避策は以下となります。

   A)、および B)はネットワークやユーザを制限させることで、リスクを低減するものとなります。C)は、影響をうけるプロセスを停止することでリスクを排除するものです。Panorama のご利用状況やお客様の環境にあわせて、対策をご検討ください。

A) **Panorama 管理インターフェースの接続元 Permitted IP アドレスを設定する、もしくは** PA シリーズやお客様環境のネットワーク機器でアクセス制御を行い、Panorama へのネットワークアクセスを信頼できるユーザとネットワークのみに制限する。

・Panorama 管理インターフェースの接続元 Permitted IP アドレス設定は以下から行えます。（Log Collector モードは CLI のみ）

WebUI：Panorama > セットアップ > インターフェース > Management > アクセス許可 IP アドレス

CLI ：> configure

 # request deviceconfig system permitted-ip <*ip/netmask*>

設定後は Panorama への Commit を実行してください。

B) Panorama の前段に PA シリーズを設置している場合、以下から選択する（両方でも可）

①App-ID “ldap”と”rmi-iiop”を利用して、信頼できないネットワークや予期しない送信元とやり取りされる LDAP トラフィックおよび RMI トラフィックをブロックさせる。

②本脆弱性に対応したシグネチャを使用して当該攻撃の検知/遮断を行う。
詳細は後述の「4. PA シリーズでの対応シグネチャについて」をご参照ください。

C) Panorama が Collector Group に含まれている場合、全ての Collector Group から Panorama を削除する。

・最初に本脆弱性が内包されているプロセスの稼働状況を以下コマンドでご確認ください。
CLI：> show system software status | match elasticsearch

結果表示例：(running の場合プロセスが稼働しています)
Process elasticsearch running (pid:xxxx)

・Collector Group からの Panorama 削除は以下から行います。
WebUI：Panorama > コレクタグループ > 任意のコレクタグループ > 全般

Panorama 設定削除後に Panorama への Commit および Collector Group への Push を実行してください。その後 Collector Group に含まれていた Panorama を再起動する必要があります。

・Panorama の再起動は以下から行えます。(Log Collector モードは CLI のみ)
WebUI：Panorama > セットアップ > 操作 > デバイスの操作 > Panorama の再起動
CLI ：> request restart system

・最後に再度プロセスの稼働状況を以下コマンドでご確認ください。
CLI：> show system software status | match elasticsearch

プロセス名 elasticsearch が表示されない場合、影響をうけるプロセスが停止されています。

(注意点)本回避策を実施後は Panorama のログ収集機能およびレポート機能が動作しなくなります。また、Collector Group から Panorama を削除した場合、Panorama に保存されている全てのログが消去されます。お客様の運用に大きな影響を及ぼす場合は、回避策 A)、B)をご検討ください。

3. 恒久対策

PAN-OS 9.0.15、9.1.12-h3、10.0.8-h8 以降へのバージョンアップをご検討ください。
※いずれも 2021/12/20(PST)にメーカリリースされております。

OS バージョンアップ手順は弊社サポートサイトのアップグレード手順書をご参照ください。
※閲覧には製品ご購入時に同梱されている資料に記載のユーザ ID/パスワードが必要となります。

・弊社サポートサイト－[ダウンロード]－[手順書]－OS 変更手順
https://csps.hitachi-solutions.co.jp/paloalto/share/download/down_procedures.html

4. **PA シリーズでの対応シグネチャについて**

PA シリーズの脅威防御機能にて CVE-2021-44228, CVE-2021-45046, CVE-2021-45105 の検知/遮断が可能となる、脆弱性防御シグネチャがリリースされております。各シグネチャの情報と内包されているコンテンツバージョンは以下表 4.1 の通りです。コンテンツは随時アップデートされており、今後、新たな対応シグネチャがリリースされることや、既存のシグネチャが更新される可能性もございますので、コンテンツバージョンを最新に保つことをご検討ください。

PA シリーズにコンテンツをインストールして、セキュリティルールにて脆弱性プロファイルを適用することで検知/遮断が可能になります。
※SSL/TLS 通信を検査する場合には SSL 復号を有効にする必要があります。

表 4.1 CVE-2021-44228, CVE-2021-45046, CVE-2021-45105 の検出と遮断に必要な情報

Threat ID	Severity	Default-Action	First Release	Last Update
91991	critical	reset-server	8498-7098	8506-7141
91994	critical	reset-server	8500-7110	8505-7134
91995	critical	reset-server	8500-7110	8505-7134
92001	critical	reset-server	8502-7118	8505-7134
92007 ※1	critical	reset-server	8504-7131	8505-7134
92012 ※2	high	reset-server	8506-7141	8506-7141

（2021/12/23 時点）

※1 Threat ID 92007 は CVE-2021-45046 のみに対応したシグネチャです。
※2 Threat ID 92012 は CVE-2021-45105 のみに対応したシグネチャです。
その他 Threat ID は CVE-2021-44228, CVE-2021-45046 に対応したシグネチャです。

5. 備考

本案内は**掲載時点での** Palo Alto Networks 社公表の情報をもとに作成しています。最新情報は以下の Security Advisories と Unit42 のブログも合わせてご参照ください。

Security Advisories

CVE-2021-44228 Impact of Log4j Vulnerabilities CVE-2021-44228, CVE-2021-45046, and CVE-2021-45105

https://security.paloaltonetworks.com/CVE-2021-44228

脅威に関する情報: Apache Log4j に新たな脆弱性(CVE-2021-44228) 実際の悪用も確認

https://unit42.paloaltonetworks.jp/apache-log4j-vulnerability-cve-2021-44228/

なお、本案内でご案内しておりますサイトに掲載されている以上の情報は開示されていません。
記載内容以上の情報については、弊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。

以上