2021 年 12 月 17 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)の Palo Alto Networks 製品への影響について（第４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)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。

記

1. CVE-2021-44228 の Palo Alto Networks 製品への影響

   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。その他製品では CVE-2021-44228 の影響を受けません。

   ※Panorama への影響について前回ご案内時点ではメーカ調査中となっておりましたが、2021/12/15(PST)時点で Panorama に影響があると公表されました。

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) 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。

B) Panorama の前段に PA シリーズを設置している場合、App-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。

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-HF、10.0.8-HF 以降へのバージョンアップをご検討ください。
※いずれも 2021/12/22(PST)にメーカリリース予定となっております。
当該 OS がメーカリリースされた際には改めてご案内いたします。

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. 備考

本案内は 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 Informational: Impact of Log4j Vulnerability CVE-2021-44228
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