２０２２年5月１３日

お客様各位

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

OpenSSL の無限ループの脆弱性(CVE-2022-0778)について（第７報）

平素は Palo Alto Networks 製品ユーザー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。この度、Palo Alto Networks 社より、OpenSSL の無限ループの脆弱性についてアナウンスされましたので、以下の通りご連絡いたします。

※太字箇所は追記もしくは更新箇所となっています。

1. 概要

複数の Palo Alto Networks 社製品に OpenSSL ライブラリが無効な証明書を解析する際に無限ループに陥り、アプリケーションへのサービス拒否(DoS)を引き起こす可能性がある脆弱性が存在しております。不正な証明書を解析した際に、検証プロセスが完了する前に無限ループに陥るため、攻撃者は本脆弱性を悪用するために検証済みの証明書を必要としません。本脆弱性の重大度は 7.5(High)となっておりますが、Cortex XDR Agent および Global Protect App においては、悪用を成功させるために中間者攻撃が必要となるため、重大度は 5.9(Medium)となります。

2. 対象のお客様

下記の表で影響を受けるバージョンをご利用されているお客様。

表 2.1 対象 OS バージョン

OS バージョン	影響を受ける	影響を受けない
PAN-OS 10.2	< 10.2.1	≧ 10.2.1
PAN-OS 10.1	< 10.1.5-h1	≧ 10.1.5-h1
PAN-OS 10.0	< 10.0.10	≧ 10.0.10
PAN-OS 9.1	< 9.1.13-h3	≧ 9.1.13-h3
PAN-OS 9.0	< 9.0.16-h2	≧ 9.0.16-h2
PAN-OS 8.1	< 8.1.23	≧ 8.1.23
Global Protect App 6.0	< 6.0.1	≧ 6.0.1
Global Protect App 5.3	< 5.3.4	≧ 5.3.4
Global Protect App 5.2	< 5.2.12	≧ 5.2.12
Global Protect App 5.1	< 5.1.11	≧ 5.1.11

Cortex XDR Agent 7.5 CE	**< 7.5.100.60642 on Windows、< 7.5.100.2276 on macOS、< 7.5.100.59687 on Linux**	**≧ 7.5.100.60642 on Windows、≧ 7.5.100.2276 on macOS、≧ 7.5.100.59687 on Linux** -
Cortex XDR Agent 7.7	**< 7.7.0.60725 on Windows、< 7.7.0.2356 on macOS、< 7.7.0.59559 on Linux**	**≧ 7.7.0.60725 on Windows、≧ 7.7.0.2356 on macOS、≧ 7.7.0.59559 on Linux**
Cortex XDR Agent 7.6	**< 7.6.2.60545 on Windows、< 7.6.2.2311 on macOS、< 7.6.2.59612 on Linux**	**≧ 7.6.2.60545 on Windows、≧ 7.6.2.2311 on macOS、≧ 7.6.2.59612 on Linux**
Cortex XDR Agent 7.5	**< 7.5.3.60113 on Windows、< 7.5.3.2265 on macOS、< 7.5.3.59465 on Linux**	**≧ 7.5.3.60113 on Windows、≧ 7.5.3.2265 on macOS、≧ 7.5.3.59465 on Linux**
Cortex XDR Agent 7.4	7.4.*	-
Cortex XDR Agent 6.1	**< 6.1.9.61370 on Windows、< 6.1.7.1690 on macOS、< 6.1.7.60245 on Linux**	**≧ 6.1.9.61370 on Windows、≧ 6.1.7.1690 on macOS、≧ 6.1.7.60245 on Linux**
Prisma Access 3.1	**Preferred,Innovation**	-
Prisma Access 3.0	Preferred,Innovation	-
Prisma Access 2.2	Preferred	-
Prisma Access 2.1	Preferred,Innovation	-

※本脆弱性の修正を含むバージョンとして PAN-OS 10.1.5-h1、9.1.13-h3 は 2022 年 4 月 7 日(PST)に、PAN-OS 10.0.10、9.0.16-h2 は 2022 年 4 月 12 日(PST)に、PAN-OS 10.2.1 は 2022 年 4 月 18 日(PST)に、PAN-OS 8.1.23 は 2022 年 4 月 28 日(PST)にメーカリリースされております。

Global Protect App 6.0.1 は 2022 年 5 月 5 日(PST)に、5.1.11 は 2022 年 5 月 13 日(PST)にメーカリリースされております。Global Protect App 5.3.4、5.2.12、は 2022 年 5 月(PST)にメーカリリース予定です。

Cortex XDR Agent 7.5.3 は 2022 年 4 月 25 日(PST)にメーカリリースされております。**Cortex XDR Agent 7.6.2-hotfix1、7.7.0-hotfix2(Windows/macOS)は 2022 年 4 月 25 日(PST)にメーカリリースされております。**7.7.0-hotfix1(Linux)では既に修正されております。**Cortex XDR Agent 6.1.9、6.1.7 および 7.5.100 CE は 2022 年 5 月 9 日(PST)にメーカリリースされております。**

Cortex XDR Agent 7.4 に関しては 2022 年 5 月 24 日にメーカサポート終了となるため修正がされない予定となります。

3. 回避策

PA シリーズの脅威防御機能にて CVE-2022-0778 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下記の表 3.1 の通りです。

表 3.1 CVE-2022-0778 の検出と遮断に必要なシグネチャ情報

Threat ID	CVE	Severity	Default-Action	First Release	Last Update
92409	2022-0778	high	reset-server	8552-7333	8552-7333
92411	2022-0778	high	reset-server	8552-7333	8552-7333
92522	**2022-0778**	**high**	**reset-client**	**8563-7374**	**8563-7374**

(2022 年 5 月 13 日時点)

※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。

4. 恒久対策

本脆弱性に対するソフトウェアアップデートとして、PAN-OS 10.1.5-h1、9.1.13-h3 が 2022 年 4 月 7 日(PST)に、PAN-OS 10.0.10、9.0.16-h2 が 2022 年 4 月 12 日(PST)に、PAN-OS 10.2.1 が 2022 年 4 月 18 日(PST)に、PAN-OS 8.1.23 が 2022 年 4 月 2

8 日(PST)にメーカリリースされております。当該バージョン以降へのバージョンアップをご検討下さい。

Global Protect App 6.0.1 が 2022 年 5 月 5 日(PST)に、5.1.11 が 2022 年 5 月 13 日(PST)にメーカリリースされております。Global Protect App 5.3.4、5.2.12 が 2022 年 5 月(PST)にメーカリリース予定です。

Cortex XDR Agent 7.5.3 が 2022 年 4 月 25 日(PST)にメーカリリースされております。**Cortex XDR Agent 7.6.2-hotfix1、7.7.0-hotfix2(Windows/macOS)が 2022 年 4 月 25 日(PST)にメーカリリースされております。**7.7.0-hotfix1(Linux)では既に修正されております。**Cortex XDR Agent 6.1.9、6.1.7 および 7.5.100 CE が 2022 年 5 月 9 日(PST)にメーカリリースされております。**

Cortex XDR Agent 7.4 に関しては 2022 年 5 月 24 日にメーカサポート終了となるため修正がされない予定となります。

具体的なバージョン等の詳細情報が公開され次第ご案内いたします。

5. その他特記事項

本脆弱性の詳細や最新情報については、下記の Palo Alto Networks 社ページも併せてご参照ください。

Security Advisories

CVE-2022-0778 Impact of the OpenSSL Infinite Loop Vulnerability CVE-2022-0778

https://security.paloaltonetworks.com/CVE-2022-0778

なお、掲載されている以上の情報は開示されておりません。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致しかねますことを予めご了承ください。

また、Palo Alto Networks 社からは、2022 年 3 月 9 日および同 31 日に本脆弱性以外にも Palo Alto Networks 社製品に関するセキュリティアドバイザリーが複数発表されております。(High 1 件、Medium 1 件、None 2 件)

これらについても上記の Security Advisories からご参照ください。　　以上