２０２２年４月６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

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。

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-hf	≧ 10.1.5-hf
PAN-OS 10.0	< 10.0.10	≧ 10.0.10
PAN-OS 9.1	< 9.1.13-hf	≧ 9.1.13-hf
PAN-OS 9.0	< 9.0.16-hf	≧ 9.0.16-hf
PAN-OS 8.1	< 8.1.23	≧ 8.1.23
Cortex XDR Agent	all	-
Global Protect App	all	-
Prisma Access 3.0	Preferred,Innovation	-
Prisma Access 2.2	Preferred	-
Prisma Access 2.1	Preferred,Innovation	-

※PAN-OS 10.2.1, 10.1.5-hf, 10.0.10, 9.1.13-hf, 9.0.16-hf, 8.1.23 は本脆弱性の修正を含むバージョンとして 2022 年 4 月にメーカリリース予定です。

3. 回避策

2022 年 4 月 6 日時点では回避策や緩和策は公開されておりません。

4. 恒久対策

2022年4月6日時点では本脆弱性に対するソフトウェアアップデートはございません。
※修正バージョンとして PAN-OS 10.2.1、10.1.5-hf、10.0.10、9.1.13-hf、9.0.16-hf、8.1.23 が 2022 年 4 月にメーカリリース予定です。
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