２０２２年８月１９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

URL Filtering における反射/増幅型 DoS 攻撃の脆弱性(CVE-2022-0028)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、URL Filtering における反射/増幅型 DoS 攻撃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

PAN-OS の URL Filtering ポリシーの設定内容によって、ネットワークベースの攻撃者が反射/増幅型の TCP サービス拒否(RDoS)攻撃を実行できる可能性がある脆弱性が存在しております。当該 DoS 攻撃は Palo Alto Networks 社製品から、攻撃者が指定したターゲットに対して実行されているように見えます。

外部攻撃者が本脆弱性を悪用するには、1 つ以上の block アクションカテゴリを含む URL Filtering プロファイルが、外部ネットワークに面したインターフェースに割り当てられた送信元ゾーンを持つセキュリティポリシーに設定されている必要があります。

※詳細については項番 3 も併せてご参照ください。

本脆弱性が悪用された場合でも、Palo Alto Networks 社製品の機密性、完全性、可用性に影響はございません。

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	< 10.2.2-h2	≧ 10.2.2-h2
PAN-OS 10.1	< 10.1.6-h6	≧ 10.1.6-h6
PAN-OS 10.0	< 10.0.11-h1	≧ 10.0.11-h1
PAN-OS 9.1	< 9.1.14-h4	≧ 9.1.14-h4
PAN-OS 9.0	< 9.0.16-h3	≧ 9.0.16-h3
PAN-OS 8.1	< 8.1.23-h1	≧ 8.1.23-h1
Prisma Access 3.1	-	All
Prisma Access 3.0	-	All

Prisma Access 2.2	-	All
Prisma Access 2.1	-	All
Cloud NGFW	-	All

※1 Panorama(M シリーズおよび VM)に影響ございません。
※2 Cloud NGFW および Prisma Access に影響ございません。

3. 影響を受ける構成かどうかの確認方法
外部攻撃者が本脆弱性を悪用するには、1 つ以上の block アクションカテゴリを含む URL Filtering プロファイルが、外部ネットワークに面したインターフェースに割り当てられた送信元ゾーンを持つセキュリティポリシーに設定されている必要があります。

以下 3 つの条件が全て当てはまる場合に影響がございますので、WebUI にて設定内容をご確認ください。

① ゾーン A（外部側）からゾーン B へのトラフィックを許可するセキュリティポリシーに、1 つ以上の block アクションカテゴリを含む URL Filtering プロファイルが設定されている。

【確認手順】
1. WebUI にアクセス
2. Policies タブから Security をクリック
3. 送信元ゾーンが外部側で設定されているポリシーを確認。
（ポリシー数が多い場合はフィルタリングをご活用ください）
4. 表示されたセキュリティポリシーのカラムを参照し、以下要件を確認
・アクション：Allow
・プロファイル:URL Filtering プロファイルアイコンの表示
（カーソルを各アイコンへ合わせることで、プロファイルの種類と合わせて、プロファイル名を参照することが可能です。）
5. Objects タブから Security Profiles > URL Filtering をクリック。
6. 4 で確認した URL Filtering プロファイルのカラム「Site Access」にて Block が設定されているかを確認

② ゾーン A（外部側）の Zone Protection プロファイルにて以下の両方が有効化されていない。

【確認手順】
Network > Network Profiles > Zone Protection
・Packet Based Attack Protection > TCP Drop > TCP Syn With Data
・Packet Based Attack Protection > TCP Drop > Strip TCP Options > TCP Fast Open

③ ゾーン A（外部側）の Zone Protection プロファイルの以下が有効化されていない。もしくは有効化されているが、Activate 閾値が 0 以外としている。

【確認手順】
Network > Network Profiles > Zone Protection
・Flood Protection > SYN > Action > SYN Cookie

4. 回避策

外部ネットワークに面したインターフェースに割り当てられた送信元ゾーンを持つセキュリティポリシーに、1 つ以上の block アクションカテゴリを含む URL Filtering プロファイルが設定されている場合、この構成を削除することで攻撃者が本脆弱性を悪用することを防ぐことができます。

本脆弱性に起因する攻撃を防ぐには、URL Filtering プロファイルが設定されているセキュリティルールが割り当てられた全てのセキュリティゾーンで、以下 2 つの Zone Protection 軽減策の内いずれかを有効にすることをご検討ください。
※両方を適用する必要はありません。

① Zone Protection プロファイルにて以下の両方を有効化する。
Network > Network Profiles > Zone Protection
・Packet Based Attack Protection > TCP Drop > TCP SYN with Data
・Packet Based Attack Protection > TCP Drop > Strip TCP Options > TCP Fast Open

② Zone Protection プロファイルにて以下を有効化する。（Activate 閾値は 0 にする）
Network > Network Profiles > Zone Protection
・Flood Protection > SYN > Action > SYN Cookie

5. 恒久対策

本脆弱性の修正バージョンである PAN-OS 10.2.2-h2, 10.1.6-h6, 10.0.11-h1, 9.1.14-h4,9.0.16-h3, PAN-OS 8.1.23-h1 が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ください。

6. 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-2022-0028 PAN-OS: Reflected Amplification Denial-of-Service (DoS) Vulnerability in URL Filtering
https://security.paloaltonetworks.com/CVE-2022-0028

以上