２０２６年5月１８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

DNS 機能における脆弱性（CVE-2026-0264)についてのお知らせ

平素は Palo Alto Networks 製品ユーザ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 DNS 機能における脆弱性（CVE-2026-0264)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 ソフトウェアの DNS プロキシおよび DNS サーバー機能におけるバッファオーバーフローの脆弱性により、攻撃者がサービス拒否(DoS)状態を引き起こすことや、攻撃者が細工したネットワークトラフィックを送信して任意のコードを実行する可能性があります。

2. 対象のお客様と対策バージョン

対象は表 1 の影響を受ける OS バージョンおよび次ページ記載の構成でご利用されているお客様です。

なお、VM シリーズ、Panorama、Cloud NGFW および Prisma Access は当該脆弱性の影響を受けません。

表 1 対象 OS バージョン

OS バージョン	影響を受ける OS バージョン	対策 OS バージョン
PAN-OS 12.1 系	12.1.5～12.1.6	12.1.7※以上
	12.1.2～12.1.4-h*	12.1.4-h5 または 12.1.7※以上
PAN-OS 11.2 系	11.2.12 未満	11.2.12※以上
	11.2.8～11.2.10-h*	11.2.10-h6 または 11.2.12※以上
	11.2.5～11.2.7-h*	11.2.7-h13 または 11.2.12※以上
	11.2.0～11.2.4-h*	11.2.4-h17※または 11.2.12※以上
PAN-OS 11.1 系	11.1.15 未満	11.1.15※以上
	11.1.11～11.1.13-h*	11.1.13-h5 または 11.1.15※以上
	11.1.8～11.1.10-h*	11.1.10-h25 または 11.1.15※以上
	11.1.7～11.1.7-h*	11.1.7-h6※または 11.1.15※以上
	11.1.5～11.1.6-h*	11.1.6-h32 または 11.1.15※以上
	11.1.0～11.1.4-h*	11.1.4-h33 または 11.1.15※以上

PAN-OS 10.2	10.2.17～10.2.18-h*	10.2.18-h6 以上
	10.2.14～10.2.16-h*	10.2.16-h7 または 10.2.18-h6 以上
	10.2.11～10.2.13-h*	10.2.13-h21 または 10.2.18-h6 以上
	10.2.8～10.2.10-h*	10.2.10-h36 または 10.2.18-h6 以上
	10.2.0～10.2.7-h*	10.2.7-h34※または 10.2.18-h6 以上

※　5/28(米国時間)にメーカリリース予定。

当該事象の影響を受けるのは、以下のいずれかの条件を満たしている構成です。

- DNS プロキシが有効かつ、DNS プロキシ設定にインターフェースが追加されている場合。

  ※NETWORK > DNS Proxy に移動して、画面上の DNS プロキシ設定一覧より、以下の項目をご確認ください。

  1. ENABLED にチェックがついている。
  2. INTERFACES に ethernet ポートが表示されている。

- PA シリーズに信頼できない DNS サーバーの IP アドレスを設定している場合。

  ※DEVICE > Setup > Services に移動して、以下の項目をご確認ください。

  1. Primary DNS Server
  2. Secondary DNS Server

  上記において、DNS Proxy Object が設定されている場合は、DNS プロキシの設定(NETWORK > DNS Proxy)で以下をご確認ください。

  1. PRIMARY DNS
  2. SECONDARY DNS

DNS プロキシの設定に関する詳細につきましては、メーカーの下記ナレッジベースをご参照ください。

How to Configure DNS Proxy on a Palo Alto Networks Firewall

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFcCAK

なお、ご参照いただくには CSP アカウントを所有している必要があります。

CSP アカウントの作成をご要望の場合は、サポートサイト> サービス> 弊社からのお知らせに掲載されている「Paloalto 個人情報取得申請フォーム」に必要事項をご記入頂き、ファイルを添付して弊社サポート窓口まで申請して下さい。

3. 回避策および緩和策

以下 2 つの対策を講じることで、本脆弱性のリスクを緩和することができます。
ご利用の設定において、以下の変更を実施することをご検討ください。

- DNS プロキシ設定に追加されているインターフェースのうち、外部ネットワークからアクセス可能なインターフェースを削除する。
  1. NETWORK > DNS Proxy に移動する。
  2. 設定を変更する DNS プロキシ設定をクリックする。
  3. INTERFACE 設定にて、該当するインターフェースをチェックして画面上の Delete をクリックする。
  4. OK をクリックして画面を閉じ、設定を Commit する。

  なお、DNS プロキシ機能を利用していない場合は、本機能を無効にして頂くことも有効です。
  1. NETWORK > DNS Proxy に移動する。
  2. 設定を無効にする DNS プロキシ設定をクリックする。
  3. 画面上の Enable のチェックを外す。
  4. OK をクリックして画面を閉じ、設定を Commit する。

- 信頼できる DNS サーバーの IP アドレスを設定する。
  1. Device > Setup > Services に移動し、画面上の歯車アイコンをクリックし、以下の項目を変更する。
     1. Primary DNS Server
     2. Secondary DNS Server

     上記において、DNS Proxy Object が設定されている場合は、DNS プロキシの設定(NETWORK > DNS Proxy)で以下の項目をご変更ください。
     1. PRIMARY DNS
     2. SECONDARY DNS

4. 解決策

対象のお客様は、表 1 の対策 OS バージョンへのアップグレードをご検討ください。

5. その他特記事項

本トピック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。

https://security.paloaltonetworks.com/CVE-2026-0264

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。

以上