

2024年8月21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

コンテンツバージョン 8880 にてリモートデスクトップサービス (RDS/RDL) に接続できなくなる問題について

平素は Palo Alto Networks 製品ユーザサポートをご利用くださり誠にありがとうございます。この度、Palo Alto Networks 社よりコンテンツバージョン 8880 にてリモートデスクトップサービス (RDS/RDL) に接続できなくなる問題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

2024年8月12日午後6時30分 (PDT) 頃、コンテンツバージョン 8880 がリリースされました。このコンテンツバージョンをインストールした後、一部のお客様にてリモートデスクトップサービス (RDS/RDL) に接続できない状態となりました。コンテンツバージョン 8880 は、2024年8月13日午前9時15分 (PDT) 時点で、お客様がダウンロードしてインストールするのを防ぐために更新サーバーから既に削除されています。また、2024年8月13日午後1時19分 (PDT) 頃、リモートデスクトップサービス (RDS/RDL) に接続できなくなる問題を引き起こしたシグネチャを含まないコンテンツバージョン 8881 がリリースされています。

2. 原因

当該事象を引き起こした脅威シグネチャ ID は 95501 です。このシグネチャは、MadLicense と呼ばれるリモートデスクトップサービス (RDS/RDL) における重大なリモートコード実行 (RCE) の脆弱性 (CVE-2024-38077) に対応するために作成されました。本来は本脆弱性を検出するために設計されていましたが、一部の無害なリモートデスクトップライセンス (DEC/RPC) トラフィックと衝突し、その結果、お客様が Windows Server でリモートデスクトップサービス (RDS/RDL) へ接続できない状態が発生しました。

3. 対応策

お客様の状況によって下記のご対応をお願い致します。

- A) コンテンツバージョン 8880 をダウンロードしていない場合**
対応不要です。当該事象の影響を受けません。

- B) コンテンツバージョン 8880 をダウンロードしたがインストールしていない場合**
スケジュール更新によって自動的にインストールされないように、PA からコンテンツバージョン 8880 を削除してください。

- C) コンテンツバージョン 8880 をインストールした場合**
コンテンツバージョン 8881 以降をダウンロードしてインストールしてください。

- D) コンテンツバージョン 8881 以降を実行している場合**
対応不要です。

以上