２０２０年１２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 製品ユーザーサポート

FireEye 社 RedTeam ツール流出における Palo Alto Networks 社製品への影響について

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。

サイバーセキュリティ企業である FireEye 社が 12 月 8 日に、攻撃診断ツール「RedTeam」が流出したことを公表しております。本件における Palo Alto Networks 社製品への影響について、以下の通りご連絡いたします。

1. 概要

   サイバーセキュリティ企業である FireEye 社が 12 月 8 日に、攻撃診断ツール「RedTeam」が流出したことを公表しております。

2. 影響について

   FireEye 社より RedTeam ツールでの攻撃に利用されている脆弱性が公表されておりますが、Palo Alto Networks 社製品のシグネチャにて検知が可能でございます。

3. 攻撃に利用されている脆弱性リストと検知シグネチャ

   以下メーカサイトの「表 2: CVE と UTID とのマッピング」に該当の脆弱性を利用した攻撃を検知することが可能なシグネチャを合わせて記載しておりますのでご参照ください。

   https://unit42.paloaltonetworks.jp/fireeye-red-team-tool-breach/

   対象のシグネチャが PA に適用済みであるかどうかは、下記の方法にてご確認いただけます。

   ■GUI 手順

   (1)[Objects]タブ > [Security Profiles] > [Vulnerability Protection]を選択し、任意のプロファイルを選択します。

   (2)[Expections]タブを選択し、"Show all signatures"にチェックを入れます。

   (3)入力フィールドにて、Thread ID を入力し検索し、検索で表示された脅威名が Thread ID と一致することを確認します。

例えば、59336 と検索し、THREAT NAME に「Microsoft Netlogon Elevation of Privilege Vulnerability」が表示される場合には対象のシグネチャが PA に適用されております。検索で表示されない場合は対象のシグネチャが PA に適用されておりません。

4. 今後の対応

Palo Alto Networks 社製品をご利用中のお客様に対し、同侵害ならびに実際に識別されたすべての脅威に対する製品組み込みの保護は継続的に更新されます。
本件の対応といたしまして各シグネチャの定期的なアップデートをお願いいたします。

以上