２０２３年１０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

カスタム App-ID を構成している場合に脅威防御チェックがバイパスされる問題について

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、カスタム App-ID を構成している場合に脅威防御のチェックがバイパスされ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

カスタム App-ID を unknown-tcp/unknown-udp トラフィックを識別するように構成している場合に、特定の脅威防御のチェックがバイパスされる問題がございます。

2. 対象のお客様

Threat Prevention (Advanced Threat Prevention)ライセンスをご利用、かつ下記条件のいずれかが当てはまるお客様が対象となります。

① カスタム App-ID を unknown-tcp トラフィックを識別するように構成している。
かつ、「他のアプリケーションに対するスキャンを続行」設定を無効にしている。
② カスタム App-ID を unknown-udp トラフィックを識別するように構成している。

カスタム App-ID の構成を確認する手順を下記に示します。

【カスタム App-ID の構成を確認する手順】

A) unknown-tcp/unknown-udp を識別するように構成されているかの確認方法。
① WebUI [OBJECTS > アプリケーション]に遷移。
② 検索ボックス右のドロップダウンより「カスタムアプリケーション」を選択。
③ 表示されたアプリケーション名をクリック。
④ 「シグネチャ」タブから設定されているシグネチャの「コンテキスト」を確認。
下記のいずれかが含まれているかを確認ください。
unknown-req-tcp-payload、unknown-rsp-tcp-payload、
unknown-req-udp-payload、unknown-rsp-udp-payload

B) 「他のアプリケーションに対するスキャンを続行」設定の確認方法。

① WebUI [OBJECTS > アプリケーション]に遷移。
② 検索ボックス右のドロップダウンより「カスタムアプリケーション」を選択。
③ 表示されたアプリケーション名をクリック。
④ 「設定」タブの「特徴」項目から「他のアプリケーションに対するスキャンを続行」のチェック状況を確認ください。

3. 恒久対策

Palo Alto Networks 社は、2023 年 10 月 17 日(PST)に Applications & Threat コンテンツ経由で修正プログラムをリリースする予定です。

なお、この修正により一部のお客様においては、カスタム App-ID に一致するトラフィックが既知の App-ID として識別される場合があります。
この影響によりセキュリティポリシーで当該 App-ID が明示的に許可されていない場合、トラフィックがブロックされる可能性がございます。
具体的には下記の条件となります。

① カスタム App-ID を unknown-tcp トラフィックを識別するように構成している。
かつ、セキュリティポリシーに脆弱性防御プロファイルが構成されていてカスタム App-ID で識別されたトラフィックを許可している。

② カスタム App-ID を unknown-udp トラフィックを識別するように構成している。
かつ、「他のアプリケーションのスキャンを続行する」設定が有効になっている。
もしくはセキュリティポリシーに脆弱性防御プロファイルが構成されていてカスタム App-ID で識別されたトラフィックを許可している。

上記の条件を満たしている場合、2023 年 10 月 17 日(PST)にリリースが予定されている Applications & Threat コンテンツへアップデートする前に、後述のメーカナレッジにて記載されている修正を適用するように Palo Alto Networks 社より案内がされております。

4. その他特記事項

最新の情報につきましては下記の Palo Alto Networks 社ページもご参照ください。

Customer Advisories
Issue in Custom App-IDs for Unknown Traffic
※閲覧にはメーカ CSP アカウントが必要となります。
https://live.paloaltonetworks.com/t5/customer-advisories/issue-in-custom-app-ids-for-unknown-traffic/ta-p/560270

メーカナレッジ
Threat Protection and Advance Threat Protection scanning is bypassed when Custom App IDs are configured for Unknown Traffic
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000XggDCAS

以上