２０２３年３月２０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

SSL Forward Proxy にて期限切れの証明書を提示してしまう事象について

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、SSL Forward Proxy にて期限切れの証明書が提示されてしまう事象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

特定の HTTPS サイト（https://login.microsoftonline.com 等）へログインする際に SSL Forward Proxy で署名された期限切れの中間 CA 証明書が提示されることで、復号ログに下記出力例のログが出力される事象が発生しております。

出力ログ例

Received fatal alert CertificateUnknown from client. CA Issuer URL: http://cacerts.digicert.com/DigiCertSHA2SecureServerCA-2.crt

また、PA シリーズがキャッシュされた古い証明書を使用していることも確認されています。

2. 対象のお客様

SSL Forward Proxy をご利用されており、かつ、PA シリーズの証明書ストアに信頼されたルート CA として構成された期限切れの中間 CA 証明書をインポートされているお客様。

※OS バージョンは全てが対象となります。

3. 根本的な原因

PA シリーズの証明書ストアに信頼されたルート CA として構成された期限切れの中間 CA 証明書が存在している状態で、サーバ側が同じサブジェクト名を持つ期限切れではない証明書チェーンを提示した場合に、証明書ストアの期限切れ証明書が SSL Forward Proxy 機能でのリーフ証明書生成に使用されてしまうことでクライアントブラウザに警告が表示されておりました。

※本事象が確認されたケースでは、DigiCert 中間 CA（DigiCertSHA2 Secure Server CA）が更新されてサーバ証明書チェーンで使用されていましたが、PA シリーズでは古い DigiCertSHA2 Secure Server CA が証明書ストアに残され、信頼されたルート CA として設定されていました。

4. 解決策

期限切れの中間 CA 証明書を削除し、認証局から最新の証明書をダウンロードして PA シリーズへインポートしてください。
その後、[デバイス] > [証明書の管理] > [証明書] > [デバイス証明書]にて「信頼されたルート CA」にチェックを入れて Commit を実施ください。

中間証明書のインポート手順については下記をご参照ください。
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-logs/repair-incomplete-certificate-chains

以上