更新 ： 2014 年 10 月 17 日
作成 ： 2014 年 10 月 17 日

株式会社ネットワールド
ネットワークソリューション課

＜SSL3.0 の脆弱性(POODLE) に関するお知らせ＞

10 月 14 日 SSLv3 の脆弱性(CVE-2014-3566)が公開されました。
本脆弱性に対する F5 ネットワークス社の確認状況と対策状況についてご連絡いたします。

【F5 製品へ影響】

SOL15702 <https://support.f5.com/kb/en-us/solutions/public/15000/700/sol15702> にて F5 ネットワークス社製品への影響、及びにワークアラウンドを掲載しております。

【本脆弱性の対象】

1. SSL Profiles に対する脆弱性

SSL Profile にて SSLv3 を許可する Cipher 設定にしていた場合に脆弱性の対象となります。
BIG-IP にて処理しているサービス向け通信となります。
(※v11.0.0 – v11.4.1、v10.0.0 – v10.2.4 では Default 設定で SSLv3 が許可されています。v11.5.0 以降は Default 設定で SSLv3 が許可されていません。)

2. Configuration utility に対する脆弱性

Web GUI(Configuration utility)への接続が脆弱性の対象となります。
BIG-IP への管理用通信となります。

【影響を受ける F5 ネットワークス社製品への対応・対策】

現状のところ、BIG-IP で SSLv3 を明示的に無効にする設定を行うことが、本脆弱性の対策となります。お客様環境によってはアプリケーション動作のために、SSLv3 を有効としている場合もあるため、SSLv3 を無効にしてもサービス影響が無いことを確認してから実施することを推奨いたします。

■ **SSL Profiles に対する対策**

SSL Profile の Cipher List から SSLv3 を拒否設定にすることで脆弱性対策することができます。詳細設定については下記 SOL をご確認ください。

- SOL13171: Configuring the cipher strength for SSL profiles (11.x)
- SOL7815: Configuring the cipher strength for SSL profiles (9.x – 10.x)

■ **Configuration utility に対する対策**

Web GUI (Configuration utility)にアクセスする際に使用する SSL Cipher List から SSLv3 を拒否設定することで脆弱性対策することができます。詳細設定については下記 SOL をご確認ください。

- SOL13405: Restricting Configuration utility access to clients using high encryption SSL ciphers (11.x)
- SOL6768: Restricting Configuration utility access to clients using high encryption SSL ciphers (9.x – 10.x)

以上