

POODLE : SSLv3.0 の脆弱性(CVE-2014-3566) 対応 リリースノート

本パッチは、POODLE : SSLv3.0 の脆弱性(CVE-2014-3566)に対応するため、SSL の設定変更を行うアップデートプログラムです。

1. 脆弱性の内容および影響範囲

SSLv3.0 には POODLE と呼ばれる脆弱性があり、第三者により SSLv3.0 の暗号化通信の一部が解読され、認証情報を窃取される可能性があります。

2. 対処方法

本パッチを適用することで Apache における SSLv3.0 の設定が無効化され、脆弱性に対応したバージョンへとアップデートされます。

3. 補足および注意事項

本パッチ適用後は SSLv3.0 での通信が無効化されます。

ご利用のブラウザにて SSLv3.0 のみを有効とされている場合は、AddPoint 管理画面へのアクセスができなくなります。アクセスする際はブラウザ側の設定で **TLSv1.0 を有効**にしてください。

以上