セキュリティアドバイザリー

GXSコミュニケーションゲートウェイは、Padding Oracle on Downloaded Legacy Encryption（POODLE：ダウングレードしたレガシー暗号通信でのパディングオラクル）に脆弱となる可能性があります。

このアドバイザリーを読んで、お客様のサイトが脆弱であるかどうかを判断し、この脆弱性を軽減する方法を学習してください。

影響を受けるシステム

- セキュアソケットレイヤー（SSL）通信プロトコル経由でファイルの送受信を行うGXSコミュニケーションゲートウェイすべて。

詳細

SSL接続を確立するためにGXSコミュニケーションゲートウェイで使用されるプロトコルは、POODLEバグに脆弱になる可能性があります(CVE-2014-3566)。POODLE攻撃は、実行するのが非常に困難で、1バイトのデータを入手するのに250回以上のトランザクションを試行する必要があります。

影響

SSLバージョン3(SSLv3)をサポートするすべてのサービスは、悪用される可能性があり、セキュリティ保護されたセッションの暗号が解読されたり、パスワードやその他の機密情報が漏えいすることが考えられます。送信側と受信側が両方ともSSLv3をサポートする場合、接続のみが脆弱になります。

注：お客様がトランスポートレイヤーセキュリティ（TLS）1.0以降をすでに使用して、GXSコミュニケーションゲートウェイにアクセスしている場合は、このセキュリティアドバイザリーに記載された問題の影響は受けません。社内アプリケーション管理者またはソフトウェアプロバイダーに問い合わせて、サービスの接続にTLS 1.0以降を使用していることを確認してください。

解決策

OpenTextはSSLを無効にして、GXSコミュニケーションゲートウェイへのアクセスを禁止します。その代わりに、OpenTextではPOODLEバグの攻撃を受けないより最新のプロトコルであるTLS1.0を使用します。修復方法はまだ検討中であり、これについては後ほど連絡します。

この変更に備え、サービスの中断を防ぐため、お客様は通信ソフトウェアをご自分で更新して、フォールバックモードのTLS(TLS 1.2、1.1、および1.0)をサポートすることを確認してください。

注：サードパーティのソフトウェアパッケージを使って当社のサービスに接続しているお客様は、担当のソフトウェアプロバイダーにすぐに連絡して、TLSがサポートされており、SSLを安全に無効化できることを確認されることを推奨します。

詳細情報

詳細については、FAQを参照するか、GXSカスタマーサポートにお問い合わせください。