NTTデータ・セキュリティ株式会社

TLS プロトコルの脆弱性（CVE-2009-3555）に関する検証レポート

2009/11/24
NTT データ・セキュリティ株式会社
辻　伸弘
松田　和之

【概要】

Transport Layer Security（以下 TLS）プロトコルのリネゴシエーション処理に脆弱性が存在することが発見されました。
TLS とは、通信の暗号化に利用されるプロトコルであり、Web サービス等でデータを暗号化して送受信するために利用されています。
この脆弱性により、MITM 攻撃（Man In The Middle 攻撃：中間者攻撃）を受ける危険性があります。
MITM 攻撃とは、暗号化された通信を行う二者の間に割り込み、通信内容を盗聴、改ざんする攻撃です。

今回、TLS プロトコルの脆弱性（CVE-2009-3555）の再現性について検証を行いました。

【影響を受けるとされているシステム】

OpenSSL 等のリネゴシエーションが有効な TLS プロトコルを利用したシステム

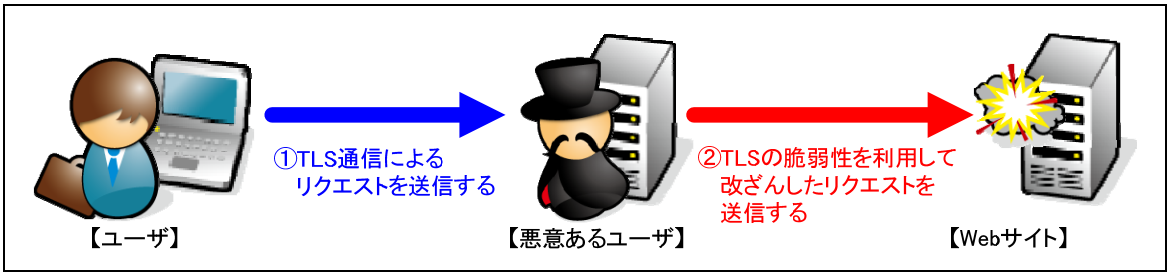
【対策案】

リネゴシエーションを無効化することが推奨されます。
なお、無効化の方法については、SSL 通信を行う各製品のベンダーサイトを参照ください。

【参考サイト】

CVE-2009-3555
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555

【検証イメージ】



【検証概要】

ターゲットのコンピュータにて、攻撃者を想定した Proxy を設定し、Proxy 経由で Twitter に書き込みを行わせることで、通信内容を改ざんし、ターゲットの Twitter ログイン情報を攻撃者の Twitter へ書き込ませます。
これにより、攻撃者は自身の Twitter の書き込みを確認することで、ターゲットの Twitter ログイン情報を取得することが可能となります。

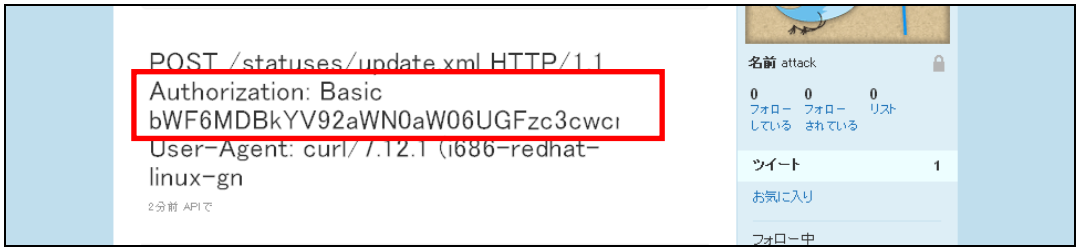
** 本脆弱性は、暗号化通信を行う二者の間の通信を盗聴できることが前提条件です。*

NTTデータ・セキュリティ株式会社

【検証結果】

下図が示すように、攻撃者の Twitter に、ターゲットのリクエスト内容が書き込まれています。
また、赤線で囲まれている部分が示すように、ターゲットの認証情報が含まれています。
これにより、リクエストの改ざんに成功し、ターゲットの Twitter ログイン情報の奪取に成功したと言えます。

ターゲットの Twitter ログイン情報の奪取に成功した画面



＊各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】
NTT データ・セキュリティ株式会社
営業企画部
TEL:03-5425-1954
http://www.nttdata-sec.co.jp/