NTT DATA
NTTデータ 先端技術株式会社

Microsoft セキュアチャネル(Schannel)におけるクライアント証明書確認の不備により任意のコードが実行される脆弱性(MS14-066)(CVE-2014-6321)に関する検証レポート

2014/12/25
NTT データ先端技術株式会社
今川　大輔

【概要】

Windows の Microsoft セキュアチャネル（Schannel）セキュリティパッケージに、リモートより任意のコードが実行される脆弱性（CVE-2014-6321）が発見されました。Schannel は複数の暗号プロトコルを実装する API です。Schannel のライブラリにおいてクライアント証明書を確認する処理に不備がありヒープバッファーオーバーフローが発生します。

攻撃者は、この脆弱性を利用することにより HTTPS を提供する Microsoft IIS や RDP（Remote Desktop Protocol）等の Schannel で暗号化されたサービスを提供する Windows Server 2003 以降の Windows OS 上でシステム停止や任意のコードを実行する可能性があります。

今回、この脆弱性（MS14-066）（CVE-2014-6321）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】

影響を受ける可能性が報告されているシステムは次の通りです。

- Windows Server 2003 Service Pack 2
- Windows Server 2003 x64 Edition Service Pack 2
- Windows Server 2003 with SP2 for Itanium-based Systems
- Windows Vista Service Pack 2
- Windows Vista x64 Edition Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for Itanium-based Systems Service Pack 2
- Windows 7 for 32-bit Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
- Windows 8 for 32-bit Systems
- Windows 8 for x64-based Systems
- Windows 8.1 for 32-bit Systems
- Windows 8.1 for 64-bit Systems
- Windows Server 2012
- Windows Server 2012 R2
- Windows RT
- Windows RT 8.1
- Windows Server 2008 for 32-bit Systems Service Pack 2（サーバー コア インストール）
- Windows Server 2008 for x64-based Systems Service Pack 2（サーバー コア インストール）
- Windows Server 2008 R2 for x64-based Systems Service Pack 1（サーバー コア インストール）
- Windows Server 2012（サーバー コア インストール）
- Windows Server 2012 R2（サーバー コア インストール）

【対策案】

Microsoft 社より、この脆弱性を修正するプログラム（MS14-066）がリリースされております。
当該脆弱性に対する修正プログラムを適用していただくことを推奨いたします。

【参考サイト】

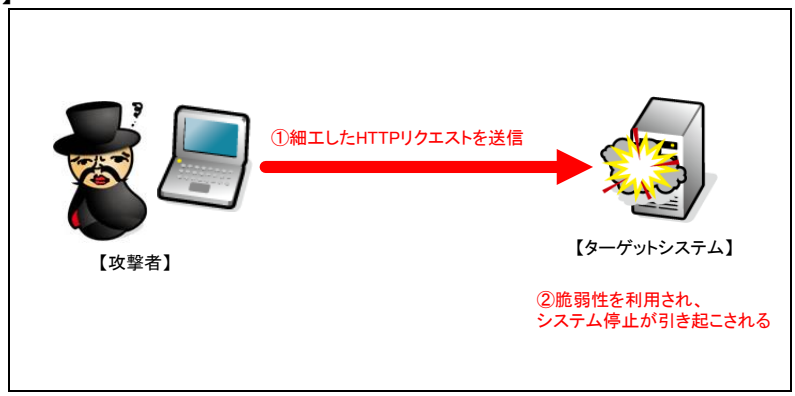
CVE-2014-6321
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6321

Schannel の脆弱性によりリモートでコードが実行される (2992611)
https://technet.microsoft.com/ja-jp/security/bulletin/ms14-066

更新：Microsoft 製品の脆弱性対策について(2014 年 11 月)
http://www.ipa.go.jp/security/ciadr/vul/20141112-ms.html

Copyright © 2014. NTT DATA INTELLILINK CORPORATION All right reserved.

【検証イメージ】

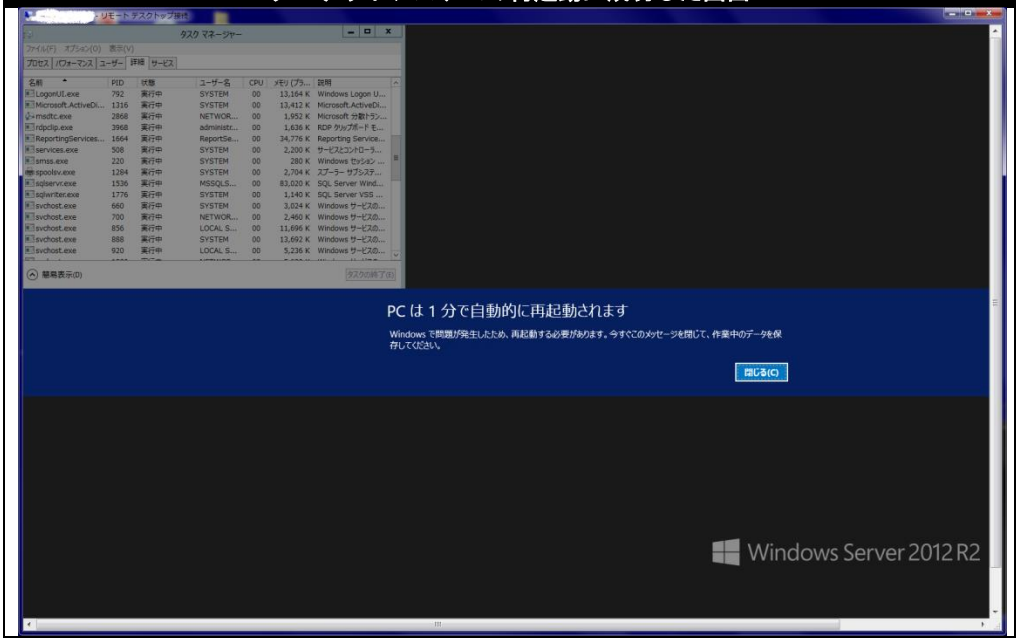


【検証ターゲットシステム】
Windows Server 2012 R2

【検証概要】
ターゲットシステムで RDP が稼動しているポートに対して、細工した SSL/TLS リクエストを送信し、ターゲットシステム上の特定のプロセス（lsass.exe）およびターゲットシステムを停止させるものです。 攻撃コードを改変することにより、リモートからターゲットシステム上で任意のコードを実行できる可能性があります。

【検証結果】
下図は、攻撃後のターゲットのシステム画面です。これにより、ターゲットシステムを再起動させることができます。

ターゲットシステムの再起動に成功した画面



＊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 データ先端技術株式会社
セキュリティ事業部
TEL:03-5859-5422
http://www.intellilink.co.jp/

Copyright © 2014. NTT DATA INTELLILINK CORPORATION All right reserved.