NTTデータ先端技術株式会社

リモートデスクトップにおける解放済みメモリを使用する脆弱性 (MS12-020)(CVE-2012-0002)に関する検証レポート

2012/3/23
NTT データ先端技術株式会社
辻 伸弘
泉田 幸宏

【概要】

リモートデスクトップに、リモートより任意のコードが実行される脆弱性が発見されました。
本脆弱性は、リモートデスクトップで利用されるプロトコル（RDP）において、細工された RDP パケットを処理する際に、メモリ内の初期化されていないオブジェクト、または、メモリより削除されたオブジェクトへアクセスすることにより発生します。

この脆弱性により、リモートからローカルユーザと同じ権限で任意のコードを実行される危険性があります。想定される被害としては、ローカルユーザ権限での情報取得、改ざん、または、ワームやスパイウェアなどの悪意あるプログラムをシステム内にインストールされることが考えられます。
なお、リモートデスクトップはデフォルトで無効化されております。

今回、この Windows の脆弱性（MS12-020）（CVE-2012-0002）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】

-Windows XP Service Pack 3
-Windows XP Professional x64 Edition Service Pack 2
-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 および Windows 7 for 32-bit Systems Service Pack 1
-Windows 7 for x64-based Systems および Windows 7 for x64-based Systems Service Pack 1
-Windows Server 2008 R2 for x64-based Systems および Windows Server 2008 R2 for x64-based Systems Service Pack 1*
-Windows Server 2008 R2 for Itanium-based Systems および Windows Server 2008 R2 for Itanium-based Systems Service Pack 1

*Server Core インストールは影響を受けます。

【対策案】

Microsoft 社より、この脆弱性を修正するプログラム（MS12-020）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。

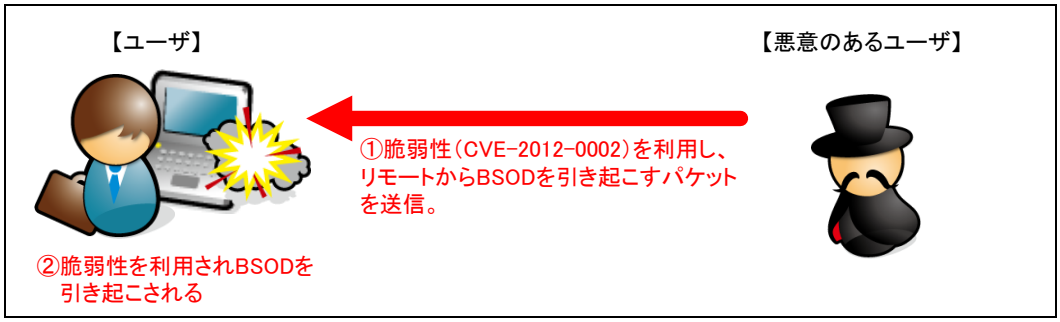
【参考サイト】

CVE-2012-0002
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002

マイクロソフト セキュリティ情報 MS12-020 - 緊急
リモート デスクトップの脆弱性により、リモートでコードが実行される (2671387)
http://technet.microsoft.com/ja-jp/security/bulletin/ms12-020

JVNDB- 2012-001760
Microsoft Windows のリモートデスクトッププロトコルの実装における任意のコードを実行される脆弱性
http://jvndb.jvn.jp/ja/contents/2012/JVNDB-2012-001760.html

【検証イメージ】

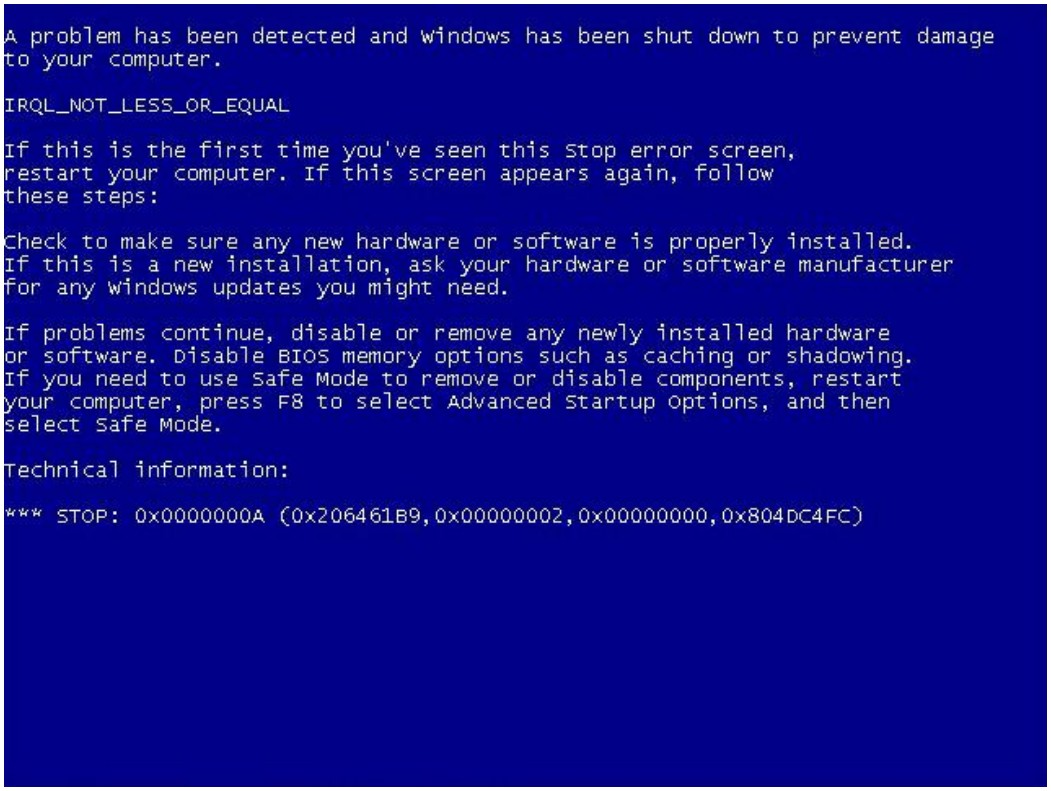


【検証ターゲットシステム】
Windows XP

【検証概要】
ターゲットシステム上で、細工した RDP パケットを送信することで BSOD（Blue Screen of Death）を引き起こすことを試みます。

【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のクラッシュ（強制終了）に成功したと言えます。

BSOD に成功した画面



NTTデータ先端技術株式会社

現時点では、リモートよりシステムの制御を奪取する攻撃コードはリリースされておりません。
一方で、今後その様なコードがリリースされる可能性は高いです。このため、早急に修正プログラム（MS12-020）を適用していただくか、Microsoft 社が推奨する回避策を行っていただくことが推奨されます。

Microsoft 社が推奨する回避策は以下のものとなります。

- 必要でない場合、ターミナルサービス、リモートデスクトップ、リモートアシスタンス、および Windows Small Business Server 2003 のリモート Web ワークプレース機能を無効化する
- ネットワーク境界に設置しているファイアウォールなどのフィルタリング機器、または Windows ファイアウォール機能で TCP/3389 番ポートをフィルタリングする
- ネットワークレベル認証機能を有効化する（ただし、Windows Vista, Windows 7, Windows Server 2008, Windows Server 2008 R2 のみ可能）

＊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　営業担当　営業企画グループ
TEL:03-5425-1954
http://security.intellilink.co.jp/