NTTデータ・セキュリティ株式会社

Windows の Embedded OpenType 処理の脆弱性(MS09-065)に関する検証レポート

2009/11/13
NTT データ・セキュリティ株式会社
辻 伸弘
松田 和之

【概要】

Microsoft 社の Embedded OpenType （以下 EOT） 処理に DoS 攻撃の脆弱性が存在することが発見されました。
EOT とは、Web ページの組み込みフォントとして用いられ、Web 閲覧者のコンピュータにフォントが組み込まれていない場合でも、指定したフォントでの表示を可能にします。
この脆弱性により、細工された Web ページの閲覧、HTML 電子メールの表示、または、電子メールの添付（細工されたフォント情報）を開いた場合に、システムをクラッシュ（強制終了）させられ、結果、BSOD(Blue Screen of Death : ブルースクリーン)を引き起こされる危険性があります。

今回、この EOT 処理の脆弱性 （MS09-065） 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 2000 SP4
Windows XP SP2 および Windows XP SP3
Windows XP Professional x64 Edition SP2
Windows Server 2003 SP2
Windows Server 2003 x64 Edition SP2
Windows Server 2003 with SP2 for Itanium-based Systems
Windows Vista SP なし、SP1、SP2
Windows Vista x64 Edition SP なし、SP1、SP2
Windows Server 2008 for 32-bit Systems SP なし、SP2
Windows Server 2008 for x64-based Systems SP なし、SP2
Windows Server 2008 for Itanium-based Systems SP なし、SP2

【対策案】

Microsoft 社から、修正プログラム （MS09-065） がリリースされています。
十分な検証の後、運用に支障をきたさないことをご確認の上、修正プログラム （MS09-065） の適用を行うことが推奨されます。
http://www.microsoft.com/japan/technet/security/bulletin/MS09-065.mspx

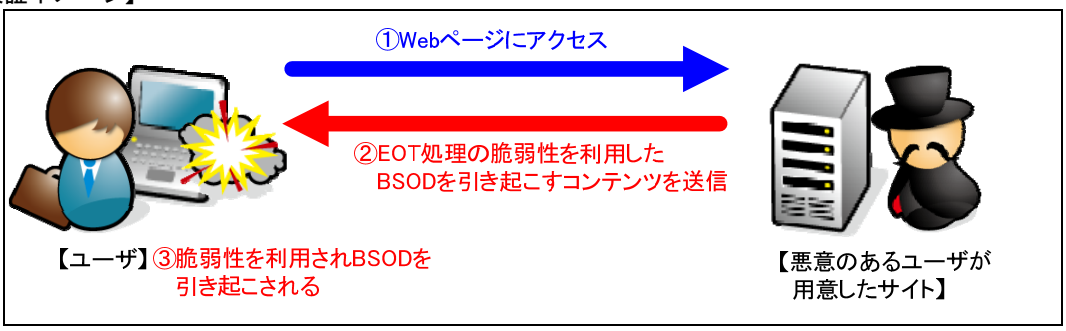
【参考サイト】

マイクロソフト セキュリティ情報 MS09-065
http://www.microsoft.com/japan/technet/security/bulletin/MS09-065.mspx

CVE-2009-2514
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2514

NTTデータ・セキュリティ株式会社

【検証イメージ】



【検証ターゲットシステム】

Windows Server 2003 SP2 日本語版
Windows XP SP3 日本語版

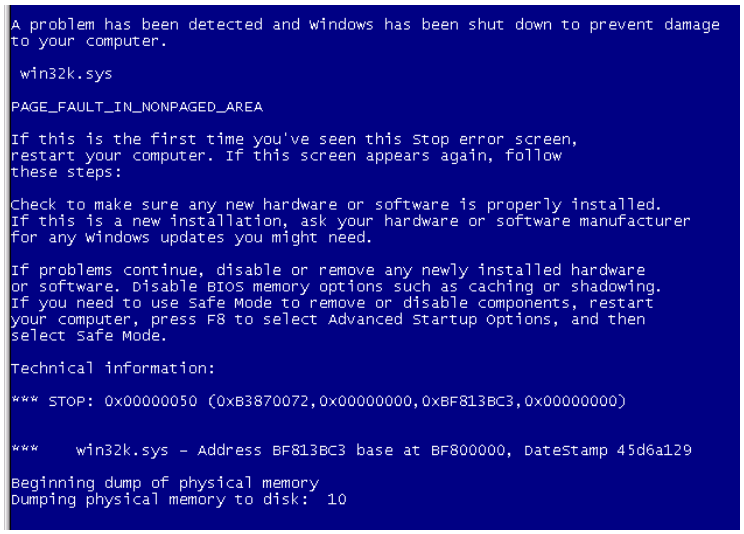
【検証概要】

ターゲットシステムに、細工した Web コンテンツをロードさせることで BSOD(Blue Screen of Death : ブルースクリーン)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システムの画面です。
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



＊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/