NTTデータ・セキュリティ株式会社

Windows の SMB（KeAccumulateTicks 関数）の DoS 攻撃の脆弱性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 SMB（Server Message Block）の KeAccumulateTicks 関数に DoS 攻撃の脆弱性が存在することが発見されました。
SMB とは、ファイル共有やプリンタ共有に利用されるプロトコルです。
この脆弱性により、システムで無限ループが発生し、システム停止を引き起こされる危険性があります。

今回、この SMB の脆弱性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 7
Windows Server 2008 R2

【対策案】

このレポート作成現在（2009 年 11 月 13 日）、修正プログラムはリリースされておりません。

本脆弱性は、SMB2 を無効にした場合にも影響を受けます。そのため回避策としては、サービスの停止ではなく、ファイアウォールなどによって通信を制限することのみが挙げられます。

【参考サイト】

マイクロソフト セキュリティ アドバイザリ (977544)
http://www.microsoft.com/japan/technet/security/advisory/977544.mspx

CVE-2009-3676
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3676

【検証イメージ】

【検証ターゲットシステム】

Windows 7 日本語版

NTTデータ・セキュリティ株式会社

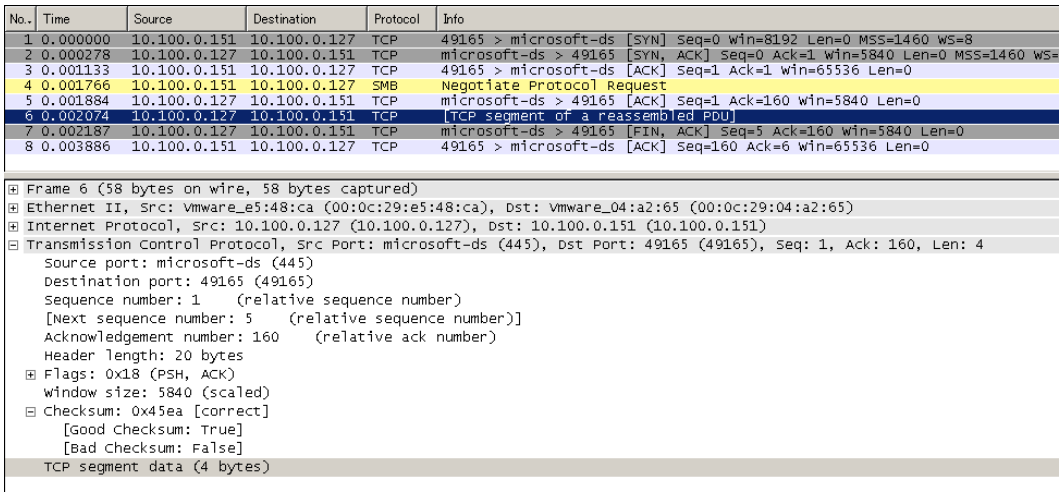
【検証概要】

ターゲットに、悪意あるユーザが用意したサイトの SMB に対して通信を要求させることで、無限ループを発生させ、システム停止を引き起こすことを試みます。

【検証結果】

下図は、実際の SMB 通信開始からターゲットシステムへの攻撃パケット送信までのパケットをキャプチャしたものです。

SMB 通信開始から攻撃パケット送信までパケットキャプチャ画面



ターゲットシステムへ攻撃パケットが送信された直後、ターゲットシステムはフリーズし、一切の操作が不能となりました。
これにより、ターゲットシステムの停止に成功したと言えます。

今回の検証では、ネットワーク共有を利用することで SMB 通信を発生させましたが、Internet Explorer でアクセスさせ、SMB 通信を発生させる攻撃方法も想定されます。また、攻撃者のブロードキャストによる攻撃方法も想定されます。

＊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/