

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】

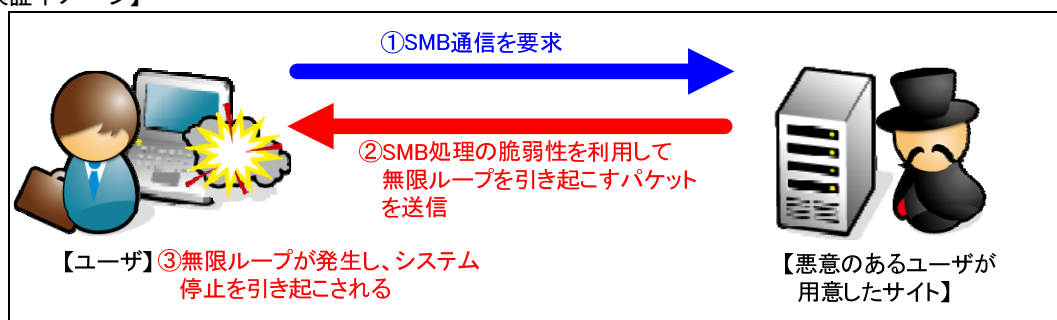
マイクロソフト セキュリティ アドバイザリ (977544)

<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

【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。

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.100.0.151	10.100.0.127	TCP	49165 > microsoft-ds [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=8
2	0.000278	10.100.0.127	10.100.0.151	TCP	microsoft-ds > 49165 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460 WS=8
3	0.001133	10.100.0.151	10.100.0.127	TCP	49165 > microsoft-ds [ACK] Seq=1 Ack=1 win=65536 Len=0
4	0.001766	10.100.0.151	10.100.0.127	SMB	Negotiate Protocol Request
5	0.001884	10.100.0.127	10.100.0.151	TCP	microsoft-ds > 49165 [ACK] Seq=1 Ack=160 win=5840 Len=0
6	0.002074	10.100.0.127	10.100.0.151	TCP	[TCP segment of a reassembled PDU]
7	0.002187	10.100.0.127	10.100.0.151	TCP	microsoft-ds > 49165 [FIN, ACK] Seq=5 Ack=160 win=5840 Len=0
8	0.003886	10.100.0.151	10.100.0.127	TCP	49165 > microsoft-ds [ACK] Seq=160 Ack=6 win=65536 Len=0


```

Frame 6 (58 bytes on wire, 58 bytes captured)
  Ethernet II, Src: Vmware_e5:48:ca (00:0c:29:e5:48:ca), Dst: Vmware_04:a2:65 (00:0c:29:04:a2:65)
  Internet Protocol, Src: 10.100.0.127 (10.100.0.127), Dst: 10.100.0.151 (10.100.0.151)
  Transmission Control Protocol, Src Port: microsoft-ds (445), Dst Port: 49165 (49165), Seq: 1, Ack: 160, Len: 4
    source port: microsoft-ds (445)
    destination port: 49165 (49165)
    sequence number: 1 (relative sequence number)
    [next sequence number: 5 (relative sequence number)]
    acknowledgement number: 160 (relative ack number)
    header length: 20 bytes
    Flags: 0x18 (PSH, ACK)
    window size: 5840 (scaled)
    checksum: 0x45ea [correct]
      [Good Checksum: True]
      [Bad Checksum: False]
    TCP segment data (4 bytes)
  
```

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/>