NTTデータ・セキュリティ株式会社

Windows の SMB の DoS 攻撃の脆弱性(CVE-2009-3103)に関する検証レポート

2009/9/9
2009/10/27(更新)
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）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、システムがクラッシュ（強制終了）させ、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 SMB の脆弱性（CVE-2009-3103）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 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】

このレポート作成現在（2009 年 9 月 9 日）、修正プログラムはリリースされておりません。

2009 年 10 月 27 日追記：
Microsoft 社から、修正プログラム（MS09-050）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（MS09-050）の適用を行うことが推奨されます。
http://www.microsoft.com/japan/technet/security/bulletin/MS09-050.mspx

修正プログラム（MS09-050）を適用したシステムに対して再度検証を行った結果、脆弱性の再現ができないことが確認されました。

本脆弱性は、SMB に接続可能であることが前提です。そのため、回避策として、SMB を無効にする、または、ファイアウォールにて接続を制限することが推奨されます。

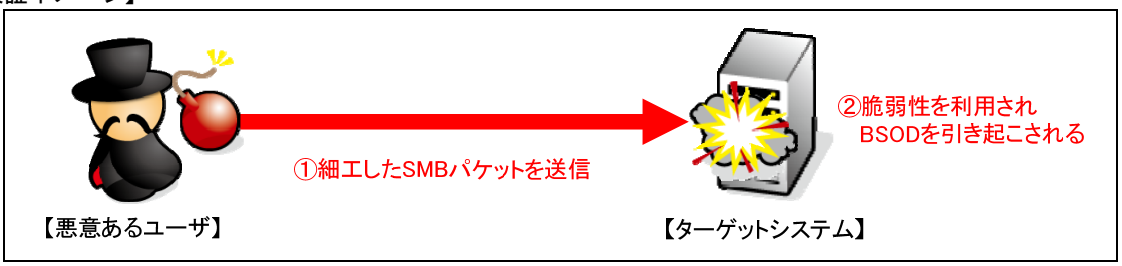
マイクロソフトセキュリティアドバイザリにて、SMB v2 を無効にする方法、ファイアウォールで TCP ポート 139、及び、445 をブロックする方法が紹介されています。
マイクロソフト セキュリティ アドバイザリ (975497)
http://www.microsoft.com/japan/technet/security/advisory/975497.mspx

【参考サイト】

CVE-2009-3103
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103

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 Vista 日本語版 （レポート作成時点フルパッチを適用）
Windows 2008 SP2 日本語版（レポート作成時点フルパッチを適用）

【検証概要】

ターゲットシステムの SMB サービスに対して、細工したパケットを送信することで、リモートからターゲットシステムをクラッシュ（強制終了）させ、結果、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。

ターゲットシステムの BSOD（Blue Screen of Death：ブルースクリーン）に成功した画面

```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

 srv2.sys

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0x9033FA70,0x00000000,0x9031E6B7,0x00000000)


***      srv2.sys - Address 9031E6B7 base at 90319000, DateStamp 49e01946


Collecting data for crash dump ...
Initializing disk for crash dump ...
```

NTTデータ・セキュリティ株式会社

＊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/