缓冲区溢出漏洞及工具收集

一、 2009 年缓冲区溢出漏洞及利用工具

Microsoft Windows CHM 文件处理缓冲区溢出漏洞

受影响系统：

Microsoft Windows XP SP3

利用工具：Exp\09-1\exp.pl

Microsoft HTML Help Workshop .hhp 文件处理缓冲区溢出漏洞

受影响系统：

Microsoft HTML Help Workshop 4.74

利用工具：Exp\09-2\exp.pl

Microsoft Windows SMB NT Trans 请求缓冲区溢出漏洞（MS09-001）

受影响系统：

Microsoft Windows XP SP3
Microsoft Windows XP SP2
Microsoft Windows Server 2003 SP2
Microsoft Windows Server 2003 SP1
Microsoft Windows 2000SP4

利用工具：Exp\09-3\ ms09001.rar

Apple iTunes 8.1.1.10 (itms/itcp) Remote Buffer Overflow Exploit (win)

利用工具：Exp\09-4\exp.py

Green Dam 3.17 (URL) Remote Buffer Overflow Exploit (xp/sp2)

利用工具：Exp\09-5\ 2009-green-dam.zip

Green Dam 3.17 URL Processing Buffer Overflow Exploit (meta)

利用工具：Exp\09-6\exp.rb

MS Internet Explorer 7 Video ActiveX Remote Buffer Overflow Exploit

利用工具：Exp\09-7\exp.rb

Mozilla Firefox 3.5 (Font tags) Remote Buffer Overflow Exploit

利用工具：Exp\09-8\exp.html

Mozilla Firefox 3.5 (Font tags) Remote Buffer Overflow Exploit (osx)

利用工具：Exp\09-9\exp.rb

二、 2008 年缓冲区溢出漏洞及利用工具

Microsoft Windows WebDAV Mini-Redirector 远程堆溢出漏洞（MS08-007）

受影响系统：

Microsoft Windows XP SP2
Microsoft Windows Vista
Microsoft Windows Server 2003 SP2
Microsoft Windows Server 2003 SP1

利用工具：Exp\08-1\exp.html

Microsoft Jet 数据库引擎 MDB 文件解析远程栈溢出漏洞(MS08-028)

受影响系统：

Microsoft msjet40.dll 4.0.8618.0
Microsoft Access 2003
Microsoft Windows XP SP2

利用工具：

Exp\08-2\ 11162007-Microsoft_Jet_Engine_MDB_File_Parsing_Exploit.rar

Microsoft Windows Media Encoder WMEX.DLL ActiveX 控件缓冲区溢出漏洞（MS08-053）

受影响系统：

Microsoft Windows Media Encoder 9 x64

Microsoft Windows Media Encoder 9

利用工具：Exp\08-3\exp.html

Microsoft SQL Server sqlvdir.dll ActiveX 控件缓冲区溢出漏洞

受影响系统：

Microsoft SQL Server 2000 SP4
Microsoft SQL Server 2000 SP3a
Microsoft SQL Server 2000 SP3
Microsoft SQL Server 2000 SP2
Microsoft SQL Server 2000 SP1
Microsoft SQL Server 2000

利用工具：Exp\08-4\exp.html

Microsoft Windows Server 服务 RPC 请求缓冲区溢出漏洞（MS08-067）

受影响系统：

Microsoft Windows XP SP3
Microsoft Windows XP SP2
Microsoft Windows Vista SP1
Microsoft Windows Vista
Microsoft Windows Server 2008
Microsoft Windows Server 2003 SP2
Microsoft Windows Server 2003 SP1
Microsoft Windows 2000SP4

利用工具：

Exp\08-5\exp-1.cpp Exp\08-5\exp-2.py Exp\08-5\ 2008-ms08-067.zip

三、 2007 年缓冲区溢出漏洞及利用工具

Microsoft Windows 矢量标记语言缓冲区溢出

漏洞（MS07-004）

受影响系统：

Microsoft Internet Explorer 7.0

Microsoft Internet Explorer 6.0 SP1

Microsoft Internet Explorer 5.0.1 SP4

Microsoft Windows XP SP2

Microsoft Windows Server 2003 SP1

Microsoft Windows Server 2003

Microsoft Windows 2000SP4

利用工具：Exp\07-1\exp.html

Microsoft Help Workshop 畸形.HPJ 文件远程栈溢出漏洞

受影响系统：

Microsoft Visual Studio 6.0 SP6

Microsoft Visual Studio 2003

Microsoft Help Workshop 4.03.0002

利用工具：Exp/07-2/exp.cpp

Microsoft Help Workshop 畸形.CNT 文件栈缓冲区溢出漏洞

受影响系统：

Microsoft Visual Studio 6.0

Microsoft Visual Studio 2003

Microsoft Help Workshop 4.03.0002

利用工具：Exp/07-3/exp.cpp

Microsoft Windows 动画光标畸形 ANI 头结构远程栈溢出漏洞(MS07-017)

受影响系统：

Microsoft Windows XP SP2

Microsoft Windows XP Professional x64 Edition

Microsoft Windows Vista

Microsoft Windows Server 2003 SP1

Microsoft Windows Server 2003

Microsoft Windows 2000SP4

利用工具：Exp/07-4/exp-1.cpp Exp/07-4/exp-2.cpp

Microsoft Word 2007 WWLib.DLL 文档处理缓冲区溢出漏洞

受影响系统：

Microsoft Word 2007

利用工具：Exp/07-5/ 04092007-0day.tar.gz

Microsoft IE Speech API 4 COM 对象实例化缓冲区溢出漏洞（MS07-033）

受影响系统：

Microsoft Internet Explorer 7.0
Microsoft Internet Explorer 6.0 SP1
Microsoft Internet Explorer 6.0
Microsoft Internet Explorer 5.0.1 SP4

利用工具：Exp/07-6/ exp-for-xp-sp2.html Exp/07-6/ exp-for-2000-sp4.html

Apple Safari for Windows 书签标题缓冲区溢出漏洞

受影响系统：

Apple Safari 3.0.2 (522.13.1)
Microsoft Windows XP SP2

利用工具：Exp/07-7/ exp.html

HP 即时支持驱动程序检查 sdd.dll 栈缓冲区溢出漏洞

受影响系统：

HP Instant Support – Driver Check < v1.5.0.3

Microsoft Windows XP SP2

利用工具：Exp/07-8/ exp.html

Microsoft IIS 5.1 远程缓冲区溢出漏洞（MS07-041）

受影响系统：

Microsoft IIS 5.1

Microsoft Windows XP SP2

不受影响系统：

Microsoft IIS 6.0

Microsoft IIS 5.0

利用工具：Exp/07-9/ exp.cpp

10. Microsoft DirectX Media SDK DXTLIPI.DLL 控件远程栈溢出漏洞

受影响系统：

Microsoft DirectX Media SDK 6.0

利用工具：Exp/07-10/ exp.html

11. MSN Messenger 视频对话堆溢出漏洞(MS07-054)

受影响系统：

Microsoft MSN Messenger 7.5

Microsoft MSN Messenger 7.0

Microsoft MSN Messenger 6.2

Microsoft Windows Messenger 8.0

利用工具：Exp/07-11/ exp_msn.rar

12. Microsoft SQL Server sqldmo.dll ActiveX 控件缓冲区溢出漏洞

受影响系统：

Microsoft SQL Server 2005 SP2

利用工具：Exp/07-12/ exp.html

四、 2006 年缓冲区溢出漏洞及利用工具

Novell eDirectory Server iMonitor 远程缓冲区溢出漏洞

受影响系统：

Novell eDirectory 8.7.3

- Microsoft
Windows NT

- Microsoft Windows 2000

利用工具：Exp/06-1/exp.rb

Microsoft Windows Media Player 插件缓冲区溢出漏洞（MS06-006）

受影响系统：

Microsoft Windows XP SP2

Microsoft Windows XP SP1

Microsoft Windows Server 2003 SP1

Microsoft Windows Server 2003

Microsoft Windows 2000SP4

利用工具：Exp/06-2/exp.pl

Microsoft Windows 路由和远程访问服务溢出漏洞（MS06-025）

受影响系统：

Microsoft Windows XP SP2

Microsoft Windows XP SP1

Microsoft Windows Server 2003 SP1

Microsoft Windows Server 2003

Microsoft Windows 2000

利用工具：Exp/06-3/exp.rb

Microsoft Windows RASMAN 服务栈溢出漏洞（MS06-025）

受影响系统：

Microsoft Windows XP SP2

Microsoft Windows XP SP1

Microsoft Windows Server 2003 SP1

Microsoft Windows Server 2003

Microsoft Windows 2000

利用工具：Exp/06-4/exp.rb

Microsoft Windows TCP/IP 协议驱动远程溢出漏洞（MS06-032）

受影响系统：

Microsoft Windows XP SP2

Microsoft Windows XP SP1

Microsoft Windows Server 2003 SP1

Microsoft Windows Server 2003

Microsoft Windows 2000

利用工具：Exp/06-5/exp.cpp

Microsoft Windows DHCP Client 服务 ACK 应答处理远程缓冲区溢出漏洞（MS06-036）

受影响系统：

Microsoft Windows XP SP2

Microsoft Windows XP SP1

Microsoft Windows Server 2003 SP1

Microsoft Windows Server 2003

Microsoft Windows 2000

利用工具：Exp/06-6/ 07212006-MS06_036_DHCP_Client.tar.gz

Microsoft IIS ASP 远程缓冲区溢出漏洞（MS06-034）

受影响系统：

Microsoft IIS 5.0

- Microsoft Windows 2000 SP4

Microsoft IIS 5.1

- Microsoft Windows XP Professional SP2

- Microsoft Windows XP Professional SP1

- Microsoft Windows XP 64-bit Edition

Microsoft IIS 6.0

- Microsoft Windows 2003

利用工具：Exp/06-7/ exp.cpp

Microsoft Windows DNS 客户端缓冲区溢出漏洞（MS06-041）

受影响系统：

Microsoft Windows XP SP2

Microsoft Windows XP SP1

Microsoft Windows Server 2003 SP1

Microsoft Windows Server 2003

Microsoft Windows 2000SP4

利用工具：Exp/06-8/ exp.py

Microsoft Windows Server 服务远程缓冲区溢出漏洞（MS06-040）

受影响系统：

Microsoft Windows XP SP2
Microsoft Windows XP SP1
Microsoft Windows Server 2003 SP1
Microsoft Windows Server 2003
Microsoft Windows 2000SP4

利用工具：Exp/06-9/ exp.rb

10. Microsoft Winsock Gethostbyname 远程缓冲区溢出漏洞（MS06-041）

受影响系统：

Microsoft Windows XP SP2
Microsoft Windows XP SP1

Microsoft Windows Server 2003 SP1

Microsoft Windows Server 2003

Microsoft Windows 2000SP4

利用工具：Exp/06-10/ exp.py

11. RealNetworks 产品多个缓冲区溢出漏洞

受影响系统：

Real Networks RealPlayer Enterprise 1.x

Real Networks RealPlayer 8.0

Real Networks RealPlayer 10.x

Real Networks RealOne Player V2

Real Networks RealOne Player V1

RedHat Enterprise Linux WS 4 Extras

RedHat Enterprise Linux WS 3 Extras

RedHat Enterprise Linux ES 4 Extras

RedHat Enterprise Linux ES 3 Extras

RedHat Enterprise Linux AS 4 Extras

RedHat Enterprise Linux AS 3 Extras

Real Networks Helix Player 1.x

RedHat Desktop 4 Extras

RedHat Desktop 3 Extras

Real Networks Rhapsody 3

利用工具：Exp/06-11/ exp.pl

相关附件都在压缩包里了。