Keeping Critical Hardware Secure

Microsoft issued more than 50 security patches during 2001. We round up the most important ones, so you can ensure that your most important workstations and servers are as secure as possible.

By Robert Schifreen

This article takes a look at most of the security patches issued by Microsoft in 2001, broken down by product rather than simply by serial number. So if you run a particular product and want to ensure that it's as stable and secure as possible, check out the patches below and decide which ones affect you most.

Although some of these patches were included in various Windows and Office service packs, though that is not always the case. If in doubt, obtain and run the patch - the installer will tell you if it needs to take no further action. Alternatively, download the automated tool from **www.microsoft.com/security**, which will automatically scan your servers and tell you which patches have been installed and which are missing. The report generated by the tool will identify patches by their serial numbers (MS01-xxx for those issued during 2001), which are included in the descriptions below.

On The Web

All of the patches here are fully described and documented on the Web. You'll find them at **www.microsoft.com/technet/security/bulletin/MS01-xxx** where xxx is the three-digit serial number mentioned below. You'll also find lots of excellent general information about security at **www.microsoft.com/security**, including details on how to lock down various Microsoft products and keep them secure.

Other handy sites dealing with IT security issues include **www.itsecurity.com**, at which you'll find the Encyclopedia of Computer Security. The site also includes an "ask the expert" page, on which you can pose security questions which are then distributed to a panel of experts. Answers are posted on the site, and the service is free of charge. There's also a superb archive of previous questions and answers, which provides a great collection of real-world experiences and advice.

Office 2000

The Web Extender Client (WEC) ships with Windows 2000 and allows Internet Explorer to view and publish files via Web folders, similar to the way that they appear in Windows Explorer. A bug in WEC means that it does not respect Internet Explorer's security settings that specify when NTLM authentication is to be performed, and instead performs it with any server that requests it. This could allow a hacker to set up a Web site which initiated an NTLM authentication session and captured the user's credentials. These credentials could then be used as the basis of a brute-force attack to recover the user's password. The problem was fixed in patch 001 (see above for details of how to locate these patches on Microsoft's Web site).

Internet Explorer

Internet Explorer 5.01 and 5.5 contain a security problem which could allow a Web page or HTML email to learn the physical location of cached content on a user's PC. This means that a hacker could launch compiled HTML containing shortcuts to executables, and those executables would run on the user's PC. The problem is fixed by patch 015.

Version 5.01, 5.5 and 6 are all affected by three problems which are fixed in patch 051. One problem is the way that IE handles URLs comprised of dotless IP addresses. In some cases, IE will fail to recognise that the address is an Internet site and will treat it as being in the intranet zone, and thus apply a higher level of trust.

Two problems which could allow a hacker to spoof trusted Web sites are fixed in patch 027. The first concerns the way that digital certificates are validated, while the second could allow an attacker to display in the IE address bar the URL of a Web site other than the one being visited. This could lull the user into a false sense of security.

A flaw was discovered in the processing which is specified for certain unusual MIME encoding types when sent within HTML emails. If a hacker creates an HTML email containing an executable attachment and then modifies the MIME header information to specify that the attachment is one of the unusual types that IE handles incorrectly, IE will launch the attachment when rendering the email without first obeying any security settings in force. You need patch 020 to fix this problem, which affects IE 5.01 and 5.5.

IE 5.1 for Mac under OS X was the subject of patch 053, which fixes an exploit that could allow a hacker to run code of their choosing on someone else's machine. Interestingly, this is one of very few Microsoft patches which apply only to Macs, indicating either that the Mac is inherently more secure or that hackers rarely target it.

Patch 055 fixes a bug in Internet Explorer 5.5 and 6.0 which could allow malicious Web sites to access all the cookies on the PCs of visitors.

Windows Scripting

The Windows Scripting Host 5.1 and 5.5 also suffer from the cached content problem described above under Internet Explorer, which patch 015 fixes.

Windows NT4 And/Or TSE

Patch 003 fixed a potential Denial of Service problem with mutexes. A mutex which controls access to a networking resource does not have the correct security permissions under NT4 Server and NT4 Terminal Server Edition. This could allow someone with local access to the machine to take control of the mutex and prevent the server from being available on the network.

The NTLM security support provider service handles NTLM authentication requests. Patch 008 fixes a problem in this service which could allow a service request from an unprivileged process to run code with Local System privileges. The problem affects all NT4 systems including Workstation, Server and Terminal Server Edition.

The PPTP service contains a problem resulting in a leak of kernel memory. An attacker could crash an NT system by continually sending packets containing a specific type of content, each of which would cause a slight memory leak. Patch 009 fixes this problem, which applies to both Workstation and Server flavours of NT4.

Patch 052 fixes a problem with Terminal Services Edition and the RDP protocol, which handles a particular series of packets incorrectly. Sending these packets to a server could crash it, requiring a reboot.

Patch 048 cures a problem in the endpoint mapper which causes it to fail on receipt of a request containing a particular type of malformed data. This presents a potential DoS (Denial of Services) loophole that could be exploited over the Internet unless port 135 is blocked by a firewall.

A problem in the NNTP service in NT4 involves a memory leak in the routine which processes news postings. Someone who sent a large number of posts could effectively hang the machine, requiring it to be rebooted. To fix this problem, you need patch 043.

A memory leak in NT4 Terminal Server Edition, in a process which handles incoming RDP data via port 3389, could allow a DoS attack if a hacker sent a large amount of traffic to that port. Patch 040 applies.

WinNT is also affected by the problem of the fraudulently-obtained Microsoft code-signing certificates detailed under Win 9x and fixed by patch 017. It is also affected by the MDAC problem (see patch 022 under Windows 9x).

"The NTLM security support provider service handles NTLM authentication requests. Patch 008 fixes a problem in this service which could allow a service request from an unprivileged process to run code with Local System privileges."

Windows 2000

An error in a catalog file which ships with Windows 2000 hotfixes was fixed in 2001 with the release of patch 005. The catalog file tells Windows 2000 the details, checksum and release dates of all fixes issued to date. An error in the file could have wrongly identified an existing patch as invalid and thus caused Windows to automatically remove it if it had been installed. The problem affected all versions of Windows 2000 except Datacenter Server.

Windows 2000 Server, Advanced Server and Datacenter Server were also all affected by a denial of service vulnerability fixed by patch 006. The implementation of RDP in Windows 2000 Terminal Service could result in a server crash if it were asked by a Terminal Service user to parse a particular sequence of data, because that sequence is not handled correctly. An attacker would not need to log into the box in order to carry out this attack - he simply has to send the correct series of packets to the RDP port on the server.

All Windows 2000 server versions, including Datacenter server, suffer from the RDP memory leak mentioned under Windows NT and fixed in patch 040.

The event viewer snap-in for Windows 2000 contains an unchecked buffer in the section of code that displays the detailed view of event records. By creating an event record with specifically malformed data in one of the fields an attacker could run code of his choice on the machine or cause the event viewer to crash. The problem affects all versions of Windows 2000 and is fixed by patch 013.

Windows 2000 is also affected by the WEC problem (patch 001), as WEC ships with Windows 2000. See the discussion of this problem in the "Office 2000" section above, or check out the Web for details of patch 001. The Office 2000 version of the patch takes precedence over the Windows version, so if you're running Office 2000 and Windows 2000 you should install the Office 2000 version of the patch.

A security context error in all versions of Windows 2000 servers, including Datacenter Server, resulted in the release of patch 007. The Network DDE agent runs using the Local System security context rather than that of the current user, possibly giving an attacker the ability to run code in the Local System context and thus gain complete control of the server.

A problem affecting all Windows 2000 domain controllers concerns the way that certain types of invalid service requests are processed. Patch 011 fixes a problem where Windows should simply drop an invalid request, however, instead it performs some resource-intensive processing and then sends a response. This could allow an attacker to mount a Denial of Service attack by continually bombarding a Win2k domain controller with such invalid service requests. The patch 011 applies to Server, Advanced Server and Datacenter Server but not Pro.

Windows 2000 Terminal Server also suffers from the RDP problem described above for WinNT and which is fixed in patch 052.

The ISAPI extension which implements the Internet Printing Protocol under Windows 2000 has a buffer overrun problem, fixed by patch 023. Also a Denial of Service vulnerability for all versions of Win2k, fixed by patch 024, can be caused by a memory leak which can be triggered when the domain controller attempts to process a certain type of invalid service request.

"A problem affecting all Windows 2000 domain controllers concerns the way that certain types of invalid service requests are processed."

A problem with the Infrared comms feature in Windows 2000 involves an unchecked buffer that could allow a hacker within infrared distance to crash all or part of a Windows 2000 server. The solution is to install patch 046.

Another Windows 2000 problem relates to the LDAP server, where a hacker could change another user's password without that user's knowledge or permission. Patch 036 applies in this case. Meanwhile, a problem with the authentication used by the SMTP service under Windows 2000 could allow a hacker to authenticate to the service using incorrect credentials. Patch 037 fixes this.

Win2k is also affected by the problem of the fraudulently-obtained Microsoft code-signing certificates detailed under Win 9x and fixed by patch 017. It is also affected by the MDAC problem (see patch 022 under Windows 9x), and the NNTP problem described under Windows NT4 (patch 043).

Windows XP

Windows XP is affected by a problem in the universal Plug and Play Service which could permit a DoS attack. Patch 054 fixes this.

Windows 9x And Me

In January 2001, someone unknown fraudulently applied for a Verisign code-signing digital certificate in the name of Microsoft Corporation. This was granted, and allowed them to sign content which would then be trusted by anyone whose computer was configured to automatically trust content signed by Microsoft. Patch 017 revokes these fraudulent certificates, and applies to Windows 95, 98 and Me.

Windows Me is also affected by the WEC problem (patch 001), as WEC ships with Windows Me. See the discussion of this problem in the "Office 2000" section above, or check out the Web for details of patch 001. The Office 2000 version of the patch takes precedence over the Windows version, so if you're running Office 2000 and Windows me you should install the Office 2000 version of the patch.

The MDAC Internet Publishing Provider provides access to WebDAV resources over the Internet. The component fails to differentiate between requests made by a user and those made by a script running in the user's browser. It therefore handles all requests in the security context of the user. This could allow a hacker to browse the user's local intranet. Patch 022 fixes the problem, which applies to Windows 95, 98 and Me.

Windows 98 and Me are affected by a problem in the universal Plug and Play Service which could permit a DoS attack. Patch 054 fixes this.

A problem with the Compressed Folders facility in Windows Me exists. The passwords used to protect folders are stored in a file on the user's system and could thus be accessed by anyone with physical access to the computer. Microsoft claims that Compressed Folders was never meant to offer robust security, merely to protect against "casual inspection". The hole can be fixed with patch 019.

Visual Studio And Visual Basic

The VB6 T-SQL debugger object that ships with Visual Studio 6 has a buffer overflow problem in the code which processes parameters for one of the object's methods. A hacker could thus cause the object to fail, or could run code of his choice on the hosting machine. The problem can be fixed by applying patch 018, which also applies to Visual Basic 6 Enterprise Edition.

Word

"By embedding a macro in a template and providing a user with an RTF document that links to it, a hacker could cause a macro to run automatically when the document was opened and without any of the usual security settings being obeyed."

By embedding a macro in a template and providing a user with an RTF document that links to it, a hacker could cause a macro to run automatically when the document was opened and without any of the usual security settings being obeyed. Patch 028 fixes this problem, which affects Word 97, 98 (Japanese and Mac versions), 2000 and 2001 (Mac). Another problem in Word affects version 2002, 2000, 97, 98 (Japan), 2001 (Mac) and 98 (Mac), and exists because it's possible to modify a Word document in such a way as to prevent any security scanner from recognising the presence of an embedded macro. The macro code will, though, still execute when required. To fix the problem you need patch 034.

IIS

In mid-2000 Microsoft issued a patch for something called the "File fragment reading via .HTR" vulnerability, which could allow a remote attacker to retrieve parts of server-side files such as .ASP scripts. This problem surfaced again in 2001, fixed by patch 004, when another related vulnerability was discovered. The problem affects IIS versions 4 and 5.

Another bug in IIS 5 relates to the way that a URL is handled if it contains certain malformed data and is of a specific length. Such URLs are parsed incorrectly by IIS and could cause a memory allocation error which would result in the failure of the IIS service. It's fixed in patch 014.

WebDAV is handled incorrectly in some cases under IIS 5. A hacker who constructs a stream of malformed WebDAV requests could perform a DoS attack on a server by consuming all CPU availability. The patch for this problem is 016.

Patch 026 fixes three problems in IIS v4 and 5, which could allow someone to run operating system commands on an affected server without permission.

Patch 044 fixes a number of IIS 4 and 5 problems, including some existing problems and five new ones. The new problems relate to potential DoS problems, buffer overruns, and more.

ISA Server 2000

The ISA Server Web Proxy service incorrectly handles a certain type of Web request if it exceeds a particular length. Deliberately making requests which exceed this length will cause the service to crash. Patch 021 fixes the problem.

Patch 045 deals with three security holes in ISA Server 2000, including two possible DoS problems, plus a scripting vulnerability that could allow a hacker to access any cookies on a user's machine.

PowerPoint

There's an unchecked buffer in the code which parses PowerPoint 97 files when they are opened. A hacker could exploit this by creating a PowerPoint file containing carefully crafted data. This could crash PowerPoint, or could allow the hacker to run code of his choice on the victim's PC, in the security context of the user. Patch 002 fixes the problem.

PowerPoint 2000 also contains the unchecked buffer mentioned above for PowerPoint 2000, which is fixed by patch 002.

Version 2000 and 2002 for Windows, and 98 and 2001 for Mac, also suffer from the macro recognition problem affected Excel, which is fixed by patch 050.

Outlook

Patch 012 fixes a problem in Outlook 98 and 2000 and Outlook Express 5. The trouble concerns the code used to process vCards, which contains an unchecked buffer. By crafting a vCard data file to contain specifically chosen data, a hacker could crash the recipient's mail client or cause the client to run code of the attacker's choice on the recipient's computer.

A particularly serious problem with Outlook 2000, 2002 and 98 is fixed by patch 038. The bug could allow a Web page to manipulate the Outlook data (stored email, calendar appointments etc) on a user's computer. The patch was first released in July 2001 but revised and updated in October. Check that you are running the latest version.

Services For Unix

SFU 2.0 contains two memory leaks which could be triggered by a user request and thus allow a DoS attack. If you're using the NFS or Telnet services in SFU 2.0 you should check out patch 039.

Excel

Excel 2000 and 2002 for Windows, and 98 and 2001 for Mac, has a problem in the way that macros are detected, thus allowing some macros to evade the built-in protection that Excel provides. Patch 050 remedies this.

"SFU 2.0 contains two memory leaks which could be triggered by a user request and thus allow a DoS attack."

SQL Server

When a client connection to a SQL server is terminated it remains cached for a short time. In some cases it is possible for one user's query to re-use a cache connection belonging to the sysadmin's account. Patch 032 fixes this problem in SQL Server 7.

SQL Server 7 and 2000 also suffer from the RPC problem mentioned under Exchange Server, and which is fixed by patch 041.

Exchange Server

Exchange Server 5.5 and 2000 has a problem with the RPC services, which do not adequately validate inputs. This could allow someone to disrupt service on an RPC server. To fix the problem you need patch 041.

Exchange 2000 Outlook Web Access will process a requested item in a user's mailbox without first checking that the folder requested actually exists. A legitimate user of the system could thus slow it down by continually requesting data from deeply-nested, non-existent directories. Patch 049 rectifies this.

Exchange 5.5 has a problem that could allow someone to enumerate the global address list (GAL) without the necessary permissions. This might allow someone to look up email aliases, for example. The problem only applies to Outlook Web Access (OWA) and is fixed by patch 047.

Exchange 2000 is also affected by the 014 patch described in the section on IIS, and the 043 patch (regarding NNTP) described under the section on NT4.

FrontPage Server Extensions

An additional component of the FrontPage Server Extensions is Visual Studio RAD Support, which allows Visual InterDev 6 users to register COM objects. A buffer overflow problem exists in this component, which could let an attacker run code of his choice on the server. Patch 035 remedies this problem.

Windows Media Player

Versions 6.4, 7.0 and 7.1 of Windows Media Player have an unchecked buffer in the code used to process Windows Media Station files, which could allow someone to run code of their choice on someone else's PC. Patch 042 fixes this problem.

A problem with version 7 of the Windows Media Player concerns a feature called "skins" which allows users to customise the look and feel of the program. A vulnerability was discovered which could allow malicious skin files (.WMZ files) to run Java code that could read and browse files on a user's computer. This code could take almost any action on a user's machine which the user himself could carry out. It can be fixed by installing patch 010 or upgrading to Media Player versions greater than 7.0.

Index Server/ Indexing Service

Patch 025 fixes two unrelated problems in Index Server 2.0 and the Windows 2000 Indexing Service, namely a buffer overrun which could allow arbitrary code to run and a weakness which could allow anyone to read "include" files residing on a Web server.

Patch 033 fixes another problem in Index Server 2.0 and the Windows 2000 Indexing Service, relating to an unchecked buffer that could allow an attacker to establish a Web connection with a server and execute code of his choice on that machine. Note that the Index Server or Indexing Service code would not need to be running for the vulnerability to exist, which makes this problem more serious than it at first appears.

Conclusion

If you support servers or workstations running any version of Windows or any major Microsoft applications, it's essential to keep an eye out for important security patches. Some are designed to fix cosmetic problems, but many fix more serious holes. Literally thousands of hackers worldwide enjoy nothing more than reading about holes in Microsoft products and then scouring the Internet for servers which have not had the patch applied. Don't let your systems be vulnerable. However there have been occasional problems with some fixes that Microsoft releases, so it pays to hang on for a few days before installing new patches, and to install the updates on a test server before using them on business-critical machines.

Having studied so many security patch details during the preparation of this article, two things are worthy of note. First, buffer overruns were first discovered more than 20 years ago so it's worrying that they are still common. Second, it is not uncommon to find, in the documentation accompanying a security patch, phrases such as "Microsoft tested Windows 2000 and Windows XP. Previous versions are no longer supported, and may or may not also be vulnerable". It seems that Microsoft is willing to use every trick in the book to get yet more revenue from upgrades, including fear.

PCNA

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews

A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers

Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software

In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs

There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.