



Cressida Technology Ltd.
TM 1 Lammas Gate, 84A Meadrow
Godalming, Surrey GU7 3HT, UK
Tel : +44 1483 23 93 00 , Fax : +44 1483 23 93 83
www.cressida.info

The logo for Ecora Software, featuring the word "ecora" in a bold, blue, lowercase sans-serif font.

ecora

A vertical photograph of a server rack with blue doors, serving as a background for the left side of the page.

25 Crucial Security Patches

**By Christopher D. Roberge, MCSE,
CCNA**

**and
Andy
Evans
Security Experts, Ecora
Software**

Top 25 Security Patches You Must Have for the Windows Environment

Introduction

The most pressing task facing IT organizations today is keeping current with the deployment of security patches, particularly in the Windows environment. The reason is simple: systems missing the latest patches are vulnerable to security breaches. Missing patches are a hacker's hall-pass through your company's mission-critical corridors.

This paper presents 25 Microsoft patches that your environment must have. Miss any of these and your infrastructure is vulnerable to costly system downtime from cyber attacks. Please note, as well, that this paper is not intended to be an inclusive list of all patches that may be needed in your environment. The only way to determine which patches are critical to your environment is through an effective patch management plan. For more information on best practices for patch management, please visit Ecora's website at www.ecora.com to download the white paper "Patch Management Best Practices."

Most of these patches have earned Microsoft's vulnerability severity rating of "Critical" or "Important." Critical describes a vulnerability whose exploitation could allow destruction of data, severe degradation of services, or the propagation of an Internet worm without user action. Important denotes a vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of user data or of the integrity or availability of processing resources.

Patch research can be a time-consuming process when done manually. Ecora Software has developed Ecora® Patch Manager 3.0, which automate the research and deployment of necessary Microsoft patches. Patch Manager 3.0 automatically installs patches and provides alerts when new patches are available. Information on additional Microsoft resources and Ecora patch products appears at the end of this paper.

Service Packs and Hotfixes

Service packs are clusters of patches that are tested and known to work well together, providing strategic support. Hot-fixes, a new file or DLL to fix a bug, offer tactical support. Software vendors usually make the installation of the latest service pack a prerequisite for ongoing support. It is strongly recommended that you keep current on service pack installation: it is the foundation of responsible, secure system management. Also, Service Packs are usually cumulative, which means that an unpatched Windows 2000 system does not have to be brought to SP1, then SP2, SP3 and then SP4, but rather SP4 only can be installed bringing the entire system up to date.

First, determine what Microsoft service packs are running on your system. You can do this manually by right-clicking on the "My Computer" icon and selecting Properties, then examining the "General" tab. Service Packs are also available for most every Microsoft product from Office 2000 through Exchange and SQL Server. Each product includes the functionality to locate service pack levels, but methods will vary.

The Top 25 Must-Have Microsoft Patches

Windows 2000

The following patches apply to the Windows 2000 operating system. In this case we see how the application of Service Pack 4 (the current service pack as of this writing) includes most of the updates specific to this OS.

Included in SP4

- 1) A cumulative patch (Q327696) for Internet Information Services is available. IIS continues to be the "hackers' choice" for attacking systems. It is critical that you stay current with the latest patches if you run IIS on any system. This cumulative hotfix includes new vulnerabilities; the most serious of which could enable an attacker's code to be run on a server. IIS has been listed as one of the "Top 20 Vulnerabilities" by SANS/FBI <http://www.sans.org/top20/> for a number of years. <http://www.microsoft.com/technet/security/bulletin/ms02-062.asp>

2) A buffer overrun condition in Microsoft Data Access Components (MDAC) could lead to arbitrary code execution by an attacker (Q329414). The MDAC has been a sore spot for Microsoft for some time. It is listed as one of the "Top 20 Vulnerabilities" by SANS/FBI <http://www.sans.org/top20/>. This new vulnerability can allow execution of the attacker's code through the HTTP server, obtaining the privilege level of the process or through Internet Explorer using the privilege level of the user. <http://www.microsoft.com/technet/security/bulletin/ms02-061.asp>

3) Windows Message Timers exist to provide a way for user processes to react to events such as keystrokes and mouse clicks. A security issue has been identified that can allow an attacker to compromise a computer and gain complete (administrative privilege) control over it. The flaw is known as the WM_TIMER Message Handler Privilege Elevation (Q328310). <http://www.microsoft.com/technet/security/bulletin/ms02-071.asp>

4) A flaw in Microsoft's implementation of the Java Virtual Machine can permit execution of attacker's code (Q810030). Eight new vulnerabilities exist, the most serious of which could enable an attacker to gain complete control over a user's system. The vulnerability affects all current Microsoft operating systems. This update supersedes previous Microsoft Java and VM implementations. <http://www.microsoft.com/technet/security/bulletin/ms02-069.asp>

5) If you use Microsoft's Point-to-Point Tunneling Protocol in server or client, you should install a hotfix (Q329834) that eliminates Denial of Service (DOS) vulnerability via an unchecked buffer. By delivering malformed PPTP control data to an unprotected system, an attacker can corrupt kernel memory and crash the system. <http://www.microsoft.com/technet/security/bulletin/ms02-063.asp>

6) Two exploits in Windows Help can allow an attacker to gain control over a user's system (Q323255). A buffer overrun in HTML Help ActiveX control or execution via a downloaded HTML help file can permit an attacker's code to run with the privilege of the current user. <http://www.microsoft.com/technet/security/bulletin/ms02-055.asp>

7 and 8) Two flaws in digital certificate handling can enable attackers to perform undesirable actions. Digital certificates are used to validate the authenticity of data in signed-applications, HTTP, email, or similar methods of communication, allowing falsification of credentials in some systems. One issue involves a certificate validation flaw that enables identity-spoofing (Q328145). <http://www.microsoft.com/technet/security/bulletin/ms02-050.asp>

A second exploit can permit a remote attacker to delete digital certificates on a user's system via HTML. This is known as the Certificate Enrollment Control Flaw (Q323172). <http://www.microsoft.com/technet/security/bulletin/ms02-048.asp>

9) One word: Blaster. The fix provided by this patch supersedes the one included in Microsoft security Bulletin [MS03-026](#) and includes the fix for the security vulnerability discussed in MS03-026, as well as three newly discovered vulnerabilities. There are three vulnerabilities in the part of RPCSS service that deals with RPC messages for DCOM activation— two that could allow arbitrary code execution and one that could result in a denial of service. An attacker who successfully exploited these vulnerabilities could be able to run code with Local System privileges on an affected system, or could cause the RPCSS Service to fail. <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms03-039.asp>

Stand-Alone Patches

10) A DOS vulnerability exists that temporarily disables a Windows 2000 domain when an attacker delivers a malformed request to the domain controller (Q287397). This patch is included in Service Pack 3 for Windows 2000, but the significance of its impact warrants its own citation. <http://www.microsoft.com/technet/security/bulletin/MS01-036.asp>

11) Two vulnerabilities have been discovered in Windows 2000 terminal servers and Windows XP where users have enabled Remote Desktop (Q324380). An attacker can readily eavesdrop on terminal

server or remote desktop sessions, compromising privacy of data, or crash an existing remote desktop sessions with malformed packets.

<http://www.microsoft.com/technet/security/bulletin/ms02-051.asp>

12) Beginning with Windows 2000, it has become possible to improve the integrity of Windows share-access SMB sessions by digitally signing all packets in a session (Q309376). A flaw in the implementation can enable an attacker to silently downgrade the SMB signing settings. Because SMB is also used for dissemination of Group Policy, the integrity of this data is compromised as a result. An attacker can add users to the local Administrators group or install and run code of their choice.

http://www.microsoft.com/security/security_bulletins/ms02-070.asp

Windows XP

The following patches apply to the Windows XP Operating System. In this case we see how the application of Service Pack 1 (the current service pack as of this writing) includes most of the updates specific to this OS.

Included in SP1a

13) The Windows Remote Access Service (RAS) provides dial-up connections among computers and networks over phone lines. A RAS overflow exists in the RAS phonebook service that allows a local user to execute code on the system with the privileges of Local System (Q318138). This is known as a privilege escalation vulnerability and requires that the attacker establish user credentials prior to exploitation.

<http://www.microsoft.com/technet/security/bulletin/ms02-029.aspx>

14) Universal Plug and Play (UPnP) allows computers to discover and use network-based devices. By sending a specifically malformed NOTIFY directive, it is possible for an attacker to overflow a buffer to run code with the privilege of the UPnP service, typically System privileges on Windows XP (Q315000).

<http://www.microsoft.com/technet/security/bulletin/ms01-059.asp>

15) A cumulative patch for Windows Media Player is available (Q320920). Fixed vulnerabilities include an exploit that allows an attacker's code to be executed, giving them control of the system. This patch has been recently updated. Microsoft advises that the patch be re-installed.

<http://www.microsoft.com/technet/security/bulletin/ms02-032.asp>

Stand-Alone Patches

16) An unchecked buffer exists in the Windows XP shell that can compromise a system (Q329390). A successful attack could allow an attacker's code to run on the computer with the privilege of the user logged in. It is exploitable through attacker's code embedded within music files, such as WMA and MP3 formats. <http://www.microsoft.com/technet/security/bulletin/ms02-072.asp>

17) Two vulnerabilities have been discovered in Windows 2000 Terminal Servers and Windows XP where users have enabled Remote Desktop (Q324380). An attacker can readily eavesdrop on terminal server or remote desktop sessions, compromising privacy of data, or crash an existing remote desktop sessions with malformed packets.

<http://www.microsoft.com/technet/security/bulletin/ms02-051.asp> (Win2K Also)

9, repeated for emphasis) One word: Blaster. This vulnerability affects Windows XP (as well as NT and 2003) so it bears repeating. The fix provided by this patch supersedes the one included in Microsoft Security Bulletin [MS03-026](#) and includes the fix for the security vulnerability discussed in MS03-026, as well as three newly discovered vulnerabilities. There are three vulnerabilities in the part of RPCSS Service that deals with RPC messages for DCOM activation— two that could allow arbitrary code execution and one that could result in a denial of service. An attacker who successfully exploited these vulnerabilities could run code with Local System privileges on an affected system, or could cause the RPCSS Service to fail.

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms03-039.asp>

SQL Server 2000

The following patches apply to Microsoft SQL 2000. In this case we see how the application of Service Pack 3a (the current service pack as of this writing) includes most of the updates specific to this product.

Included in SP 3a

18) Lest we forget the Slammer Worm, (Q814372) we must point you to the following update for your SQL Servers. Early in 2003, networks worldwide were crippled by this nasty worm that managed to spread itself worldwide in less than 10 minutes. Sadly, the vulnerability which made this possible had been fixed by Microsoft 184 days earlier. Considered low-priority by many administrators, the patch was left unapplied, leaving systems vulnerable. This patch has since been rolled up into SQL SP3a.

<http://support.microsoft.com/?kbid=814372>

19) and 20) If you operate a Microsoft SQL Server database, you should install a recent hotfix to repair an exploit known as the SQL Hello Overflow. An attacker can use this flaw to execute commands against the remote host as LOCALSYSTEM, as well as read your database content. To repair this vulnerability, Microsoft recommends that you apply an update to the latest service pack, identified below for each version of SQL. Microsoft SQL is listed as one of the "Top 20 Vulnerabilities" by SANS/FBI: <http://www.sans.org/top20/>.

Q316333 SQL Server 2000 Security Update for Service Pack 3a

<http://www.microsoft.com/technet/security/bulletin/ms02-056.asp>

Download:

http://download.microsoft.com/download/SQLSVR2000/Patch/8.00.0686/W98NT42KMeXP/EN-US/8.00.0686_enu.exe

Q327068 SQL Server 7.0 Security Update for Service Pack 4

<http://www.microsoft.com/technet/security/bulletin/ms02-061.asp>

Download: http://download.microsoft.com/download/sql70/Patch/7.00.1076/WIN98MeXP/EN-US/7.00.1076_enu.exe

21) When SQL Service Packs 1, 2, or 3 are applied to a Microsoft SQL server, a blank password can be assigned or a clear-text password storage file created for the default "sa" account (Q263968). An attacker can use this flaw to execute commands against the remote host or read your database content. <http://www.microsoft.com/technet/security/bulletin/MS00-035.asp>

Exchange 2000

The following patches apply to Microsoft Exchange 2000. In this case we see how the application of Service Pack 3 (the current service pack as of this writing) includes the update specific to this product.

22) In Exchange 2000 Server, a security vulnerability exists that could allow an unauthenticated attacker to connect to the SMTP port on an Exchange server and issue a specially-crafted extended verb request. That request could cause a denial of service that is similar to the one that could occur on Exchange 5.5. Additionally, if an attacker issues the request with carefully chosen data, the attacker could cause a buffer overrun that could allow the attacker to run malicious programs of their choice in the security context of the SMTP service.

<http://www.microsoft.com/technet/security/Bulletin/MS03-046.asp>

Office 2000 and XP

The following patches apply to Microsoft Office 2000 and XP. The current Service Packs are Office 2000 Service Pack 3, and Office XP Service pack 2. Both Service Packs contain critical updates, however the three patches below are also critical.

23) There were three Office updates released in September of 2003, post SP3 that require patching. The first is a vulnerability that concerns a hacker's ability to run arbitrary code within an embedded macro in Word. A vulnerability exists because it is possible for an attacker to craft a malicious document that will bypass the macro security model. If the document was opened, this flaw could allow a malicious macro embedded in the document to be executed automatically, regardless of the level at which macro security is set.

<http://www.microsoft.com/technet/security/Bulletin/MS03-035.asp>

24) There is a flaw in the way that the Microsoft WordPerfect converter handles Corel® WordPerfect documents. A security vulnerability results because the converter does not correctly validate certain parameters when it opens a WordPerfect document, which results in an unchecked buffer. As a result, an attacker could craft a malicious WordPerfect document that could allow code of their choice to be executed if an application that used the WordPerfect converter opened the document.

<http://www.microsoft.com/technet/security/Bulletin/MS03-036.asp>

25) A flaw exists in the way VBA checks document properties passed to it when a document is opened by the host application. A buffer overrun exists which if exploited successfully could allow an attacker to execute code of their choice in the context of the logged on user.

<http://www.microsoft.com/technet/security/Bulletin/MS03-037.asp>

Installing these 25 patches will go a long way towards securing your Microsoft environment. Unfortunately, attackers never sleep and new patches are issued each week. Install an automated patch management solution to ensure that your Microsoft product and system patches are current. Ecora provides Ecora Patch Manager, which automates all aspects of patch discovery and remediation (installation) from one administrative desktop. It is available for download at <http://www.ecora.com/ecora/register/default.asp>.

For More Information:

Technical details for each patch can be found in associated Microsoft Knowledge Base Articles. An article identifier, for example "324929" accompanies each patch description. The articles are retrievable by appending the six-digit identifier to the following URL:

<http://support.microsoft.com/?kbid=>

Microsoft also maintains a library of detailed security bulletins that generally contain more thorough details about each vulnerability and its effect on the Microsoft product in question. The security bulletins can be researched individually through the URLs and identifiers provided in this paper, for example "MS02-068". Similar to Knowledge Base articles, a URL can be constructed for this security bulletin with this identifier by entering in the following fashion:

<http://www.microsoft.com/technet/security/bulletin/MS02-068.asp>

All of the above links are available within Ecora's Patch Manager 3.0. For more information on Ecora's line of risk management solutions, please visit www.ecora.com.

© 2004 Ecora Software Corporation. All rights reserved.

Novell is a registered trademark of Novell, Inc. Cisco is a registered trademark of Cisco Systems. Solaris is a trademark of Sun Microsystems, Inc. Microsoft, MS-SQL, and Windows NT are registered trademarks of the Microsoft Corporation. Oracle is a registered trademark of Oracle Corporation. Lotus and Domino are trademarks of Lotus Corporation. Ecora is a registered trademark of Ecora Software Corporation.



*Supplied by the permission of Ecora Software.