

Microsoft October 2004 Security Bulletins

Briefing for Senior IT Managers

updated October 20, 2004

Marcus H. Sachs, P.E.
The SANS Institute
October 12, 2004
<http://isc.sans.org>



Summary of October 2004 Security Bulletins

MS04-029 Vulnerability in RPC Runtime Library Could Allow Information Disclosure and Denial of Service (873350)

IMPORTANT

MS04-030 Vulnerability in WebDav XML Message Handler Could Lead to a Denial of Service (824151) **IMPORTANT**

MS04-031 Vulnerability in NetDDE Could Allow Remote Code Execution (841533) **IMPORTANT**

MS04-032 Security Update for Microsoft Windows (840987)

CRITICAL

MS04-033 Vulnerability in Microsoft Excel Could Allow Remote Code Execution (886836) **CRITICAL**

Summary of October 2004 Security Bulletins (2)

- MS04-034 Vulnerability in Compressed (zipped) Folders
Could Allow Remote Code Execution (873376) **CRITICAL**
- MS04-035 Vulnerability in SMTP Could Allow Remote Code
Execution (885881) **CRITICAL**
- MS04-036 Vulnerability in NNTP Could Allow Remote Code
Execution (883935) **CRITICAL**
- MS04-037 Vulnerability in Windows Shell Could Allow
Remote Code Execution (841356) **CRITICAL**
- MS04-038 Cumulative Security Update for Internet Explorer
(834707) **CRITICAL**

October Overview

	98/ ME	NT	2K	XP	2003	Exch Serv	Remote Code Execution	Worm Potential	Exploit Code
MS04-29		✓							
MS04-30			✓	✓	✓				✓
MS04-31	✓	✓	✓	✓	✓		✓	LOW	
MS04-32	✓	✓	✓	✓	✓		✓		✓
MS04-33	*	*	*	*	*		✓		
MS04-34				✓	✓		✓	LOW (virus)	
MS04-35				✓	✓	✓	✓		
MS04-36		✓	✓		✓	✓	✓	LOW	✓
MS04-37	✓	✓	✓	✓	✓		✓		
MS04-38	✓	✓	✓	✓	✓		✓		✓

What is MS04-029?

- A bulletin from Microsoft concerning a vulnerability that exists when the RPC Runtime Library processes specially crafted messages
 - An attacker who successfully exploited this vulnerability could potentially read portions of active memory or cause the affected system to stop responding
- Workarounds are available until patching is complete

What happens if I do nothing?

- Any anonymous user who can deliver a series of specially crafted messages to an affected system could attempt to exploit this vulnerability
 - By default, this ability is enabled on the affected systems
 - Any user who can establish a connection to an affected system could attempt to exploit this vulnerability
- An attacker may be able to exploit this vulnerability over the Internet

- 
- Remote Denial of Service
 - Information Disclosure



What systems are affected?

Affected systems:

- Microsoft Windows NT Server 4.0 Service Pack 6a
- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6

Systems NOT affected

- Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP and Microsoft Windows XP Service Pack 1
- Microsoft Windows XP Service Pack 2
- Microsoft Windows XP 64-Bit Edition Service Pack 1
- Microsoft Windows XP 64-Bit Edition Version 2003
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 64-Bit Edition
- Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

What can I do about it?

- The best solution is to download the proper update (patch) from Microsoft and install it
- Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter
- Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed

If I cannot patch, what other workarounds can I do?


- Microsoft has tested these workarounds:
 - Block the following at the network firewall:
 - UDP ports 135, 137, 138, and 445, and TCP ports 135, 139, 445, and 593
 - All unsolicited inbound traffic on ports greater than 1024
 - Any other specifically configured RPC port
 - If installed, COM Internet Services (CIS) or RPC over HTTP, which listen on ports 80 and 44
 - Enable advanced TCP/IP filtering on systems that support this feature
- Each of these workarounds will reduce the functionality of the computer
- Additional details are in the Microsoft bulletin

What is MS04-030?

- A bulletin from Microsoft concerning a vulnerability that could allow an attacker to send a specially crafted WebDAV request to a server that is running IIS and WebDAV
 - An attacker could cause WebDAV to consume all available memory and CPU time on an affected server
 - The IIS service would have to be restarted to restore functionality
- Workarounds are available until patching is complete

What happens if I do nothing?

- Any user who could deliver a WebDAV request to an affected Web server could exploit the vulnerability
 - Because WebDAV requests travel over the same port as HTTP (typically port 80), an attacker who could establish a connection to an affected Web server could try to exploit the vulnerability
- Servers running both IIS and WebDAV services are primarily at risk from this vulnerability
- An attacker may be able to exploit this vulnerability over the Internet



**Working
exploit code is
in the wild**



• Remote Denial of Service



What systems are affected?

Affected systems:

- Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP and Microsoft Windows XP Service Pack 1
- Microsoft Windows XP 64-Bit Edition Service Pack 1
- Microsoft Windows XP 64-Bit Edition Version 2003
- Microsoft Windows Server™ 2003
- Microsoft Windows Server 2003 64-Bit Edition

Systems NOT affected

- Microsoft Windows XP Service Pack 2
- Microsoft Windows NT Server 4.0 Service Pack 6
- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
- Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (Me)



What can I do about it?

- The best solution is to download the proper update (patch) from Microsoft and install it
- There are some mitigating factors that limit the impact of this issue
 - The vulnerability can only be exploited remotely if an attacker can establish a Web session with an affected server
 - By default, Windows XP and Windows Server 2003, except for Windows Server 2003 Web Server Edition, do not install IIS
 - IIS 5.0, which is included as part of Windows 2000, is the only version that enables WebDAV by default

If I cannot patch, what other workarounds can I do?

- Microsoft recommends only one workaround:
 - Disable WebDAV on IIS 5.0 if it is not needed
- This workaround will reduce the functionality of the web server
- Additional details are in the Microsoft bulletin

What is MS04-031?

- A bulletin from Microsoft concerning a vulnerability in the NetDDE services because of an unchecked buffer
 - An attacker who successfully exploited this vulnerability could take complete control of an affected system
 - The NetDDE services are not started by default and would have to be manually started for an attacker to attempt to remotely exploit this vulnerability
 - This vulnerability could also be used to attempt to perform a local elevation of privilege or remote denial of service
- Workarounds are available

What happens if I do nothing?

- After a NetDDE service is started, an attacker could exploit the vulnerability by creating and sending a specially crafted message an affected system
 - This might cause the affected system to remotely execute code
 - Receipt of such a message could also cause the vulnerable system to fail and cause a denial of service condition
- To exploit this vulnerability for a local privilege elevation, an attacker would first have to log on to the system
 - An attacker could then run a specially-designed application that could attempt to exploit the vulnerability and thereby gain complete control over the affected system.
- There is a low probability that an Internet worm might result from exploitation of this vulnerability

- Remote Code Execution
- Local Privilege Escalation
- Remote Denial of Service



What systems are affected?

Affected systems:

- Microsoft Windows NT Server 4.0 Service Pack 6a
- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
- Microsoft Windows 2000 SP3 and Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP and Microsoft Windows XP Service Pack 1
- Microsoft Windows XP 64-Bit Edition Service Pack 1
- Microsoft Windows XP 64-Bit Edition Version 2003
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 64-Bit Edition
- Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

Systems NOT affected

- Microsoft Windows XP Service Pack 2



What can I do about it?

- The best solution is to download the proper update (patch) from Microsoft and install it
- There are some mitigating factors that limit the impact of this issue
 - On Windows Server 2003 the NetDDE services are disabled by default
 - An attacker would first have to change the startup type from Disabled, and then start the service to attempt to exploit this vulnerability
- Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter

If I cannot patch, what other workarounds can I do?


- Microsoft recommends two workarounds:
 - Disable the NetDDE services via the Control Panel or Group Policy settings
 - Block the following at the firewall:
 - UDP ports 135, 137, 138, and 445, and TCP ports 135, 139, 445, and 593
 - All unsolicited inbound traffic on ports greater than 1024
 - Any other specifically configured RPC port
- If the NetDDE services are disabled, messages from NetDDE applications are not transmitted
 - If the NetDDE services are disabled, any services that explicitly depend on the NetDDE services will not start
 - An error message is logged in the system event log
- Additional details are in the Microsoft bulletin

What is MS04-032?

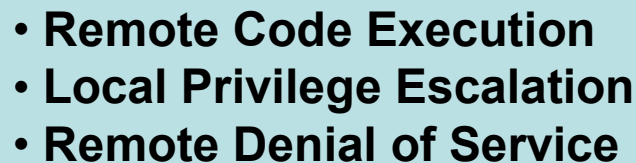
- A bulletin from Microsoft concerning four vulnerabilities in Windows:
 - Window Management application programming interfaces, local privilege escalation
 - Virtual DOS Machine subsystem, local privilege escalation
 - Graphics rendering engine, remote code execution
 - Windows kernel, local denial of service
- No workarounds available for three of these
 - Patching is the only option

What happens if I do nothing?

- An attacker who successfully exploited one or more of these vulnerabilities could take complete control of an affected system, including
 - Installing programs
 - Viewing, changing, or deleting data
 - Creating new accounts that have full privileges
- This vulnerability could also be used to attempt to perform a local elevation of privilege or a remote denial of service



**Working
exploit code is
in the wild**

- 
- Remote Code Execution
 - Local Privilege Escalation
 - Remote Denial of Service

What systems are affected?

Affected systems:

- Microsoft Windows NT Server 4.0 Service Pack 6a
- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
- Microsoft Windows 2000 SP3 and Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP and Microsoft Windows XP Service Pack 1
- Microsoft Windows XP 64-Bit Edition Service Pack 1
- Microsoft Windows XP 64-Bit Edition Version 2003
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 64-Bit Edition
- Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

Systems NOT affected

- Microsoft Windows XP Service Pack 2



What can I do about it?

- The best solution is to download the proper update (patch) from Microsoft and install it
- There are some mitigating factors that limit the impact of these issues
 - For the Windows Management and Virtual DOS Machine vulnerabilities, an attacker must have valid logon credentials and be able to logon locally to exploit this vulnerability
 - The vulnerability could not be exploited remotely or by anonymous users
 - The Graphics Rendering Engine vulnerability could be exploited by an attacker who persuaded a user to open a specially crafted file or to view a folder that contains the specially crafted image
 - There is no way for an attacker to force a user to open a malicious file, except potentially through previewing an email message

If I cannot patch, what other workarounds can I do?

- Only one of the four vulnerabilities (graphics rendering engine) has a workaround
 - Read e-mail messages in plain text format if you are using Outlook 2002 or later, or Outlook Express 6 SP1 or later, to help protect yourself from the HTML e-mail attack vector
- The remaining three have no workarounds
 - Patching is the only option
- This single workaround will reduce the functionality of the computer
- Additional details are in the Microsoft bulletin

What is MS04-033?

- A bulletin from Microsoft concerning a vulnerability in Excel
 - If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of the affected system
 - The vulnerability cannot be exploited automatically through e-mail - for an attack to be successful through e-mail, a user must open an attachment that is sent in an e-mail message
- No workarounds available
 - Patching is the only option

What happens if I do nothing?

- An attacker could host a malicious Excel file on a web site and persuade a user to click a link to the file
- The file could then be executed allowing the attacker to execute code of their choice including
 - Installing programs
 - Viewing, changing, or deleting data
 - Creating new accounts with full privileges
- An attacker could also attempt to exploit the vulnerability by sending a specially crafted file in email

What systems are affected?

Affected systems:

- Microsoft Office 2000 Service Pack 3
 - Excel 2000
- Microsoft Office XP Service Pack 2
 - Excel 2002
- Microsoft Office 2001 for Mac
 - Excel 2001 for Mac
- Microsoft Office v. X for Mac
 - Excel v. X for Mac

Systems NOT affected

- Microsoft Office XP Service Pack 3
- Microsoft Office Excel 2003
- Microsoft Office 2003 Service Pack 1
- Microsoft Excel 2004 for Mac

What can I do about it?

- The best solution is to download the proper update (patch) from Microsoft and install it
- There are some mitigating factors that limit the impact of this issue
 - In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to exploit this vulnerability
 - An attacker would have no way to force users to visit a malicious Web site
 - The vulnerability can not be exploited automatically through e-mail
 - For an attack to be successful through e-mail, a user must open an attachment that is sent in an e-mail message

If I cannot patch, what other workarounds can I do?

- There are no workarounds for this issue
 - Patching is the only option
- Additional details are in the Microsoft bulletin

What is MS04-034?

- A bulletin from Microsoft concerning a vulnerability in compressed (zipped) folders because of an unchecked buffer that handles specially crafted compressed files
 - An attacker could exploit the vulnerability by constructing a malicious compressed file that could potentially allow remote code execution if a user visited a malicious Web site
 - An attacker who successfully exploited this vulnerability could take complete control of an affected system
 - User interaction is required to exploit this vulnerability
- Workarounds are available

What happens if I do nothing?

- An attacker could host a malicious Web site and then persuade a user to view that Web site
 - An attacker could also create an e-mail message that contains a specially crafted link, and then persuade a user to view the e-mail message and then click the link
 - An attacker could also send a specially crafted zipped file to a user and then persuade the user to open the file
- There is a low probability that an attacker could create an e-mail based virus using this vulnerability



What systems are affected?

Affected systems:

- Microsoft Windows XP and Microsoft Windows XP Service Pack 1
- Microsoft Windows XP 64-Bit Edition Service Pack 1
- Microsoft Windows XP 64-Bit Edition Version 2003
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 64-Bit Edition

Systems NOT affected

- Microsoft Windows NT Server 4.0 Service Pack 6a
- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
- Microsoft Windows 2000 SP3 and Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 2
- Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)



What can I do about it?

- The best solution is to download the proper update (patch) from Microsoft and install it
- There are some mitigating factors that limit the impact of this issue
 - In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to exploit this vulnerability
 - An attacker would have no way to force users to visit a malicious Web site
 - By default, Outlook Express 6, Outlook 2002, and Outlook 2003 open HTML e-mail messages in the Restricted sites zone
 - Outlook 98 and Outlook 2000 open HTML e-mail messages in the Restricted sites zone if the Outlook E-mail Security Update has been installed

If I cannot patch, what other workarounds can I do?

- Microsoft has tested these workarounds:
 - Remove the registration for Compressed (zipped) Folders
 - Install Outlook E-mail Security Update if you are using Outlook 2000 SP1 or earlier
 - Read e-mail messages in plain text format if you are using Outlook 2002 or later
 - Do not open or save .zip files that you receive from untrusted sources
- Each of these workarounds will reduce the functionality of the computer
- Additional details are in the Microsoft bulletin

What is MS04-035?

- A bulletin from Microsoft concerning a vulnerability in the Windows Server 2003 SMTP component in the way that it handles Domain Name System (DNS) lookups
 - An attacker could exploit the vulnerability by causing the server to process a particular DNS response that could potentially allow remote code execution
 - An attacker who successfully exploited this vulnerability could take complete control of an affected system
- Workarounds are available

What happens if I do nothing?

- On Exchange Server 2003, or on systems that use the Windows Server 2003 SMTP component, an anonymous user could deliver a specially crafted DNS response message to the affected system and exploit this vulnerability
 - An attacker could then cause the affected system to execute code of the attacker's choice
 - The attacker could also cause the SMTP component and other services that are hosted by Internet Information Services on the same system to repeatedly fail

- Remote Code Execution
- Remote Denial of Service



What systems are affected?

Affected systems:

- Microsoft Windows XP 64-Bit Edition Version 2003
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 64-Bit Edition
- Microsoft Exchange Server 2003 and Microsoft Exchange Server 2003 Service Pack 1 when installed on Microsoft Windows Server 2003 (uses the Windows 2003 SMTP component)
- Microsoft Exchange Server 2003 when installed on Microsoft Windows 2000 Service Pack 3 or Microsoft Windows 2000 Service Pack 4

Systems NOT affected

- Microsoft Windows NT Server 4.0 Service Pack 6a
- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6

(continued on next slide)



What systems are affected? (2)

Systems NOT affected (continued)

- Microsoft Windows 2000 SP3 and Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP, Microsoft Windows XP Service Pack 1, and Microsoft Windows XP Service Pack 2
- Microsoft Windows XP 64-Bit Edition Service Pack 1
- Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)
- Microsoft Exchange Server 5.0 Service Pack 2
- Microsoft Exchange Server 5.5 Service Pack 4
- Microsoft Exchange 2000 Server Service Pack 3
- Microsoft Exchange Server 2003 Service Pack 1 when installed on Microsoft Windows 2000 Service Pack 3 or Microsoft Windows 2000 Service Pack 4

What can I do about it?

- The best solution is to download the proper update (patch) from Microsoft and install it
- There are some mitigating factors that limit the impact of this issue
 - By default, the SMTP component is not installed on Windows Server 2003, Windows Server 2003 64-Bit Edition, or Windows XP 64-Bit Edition Version 2003
 - By default, the SMTP component is not installed when Internet Information Services (IIS) 6.0 is installed
 - Windows NT Server 4.0, Windows 2000, Windows XP, Windows XP 64-Bit Edition, Exchange Server 5.0, Exchange Server 5.5, and Exchange 2000 Server are not affected by this vulnerability

If I cannot patch, what other workarounds can I do?

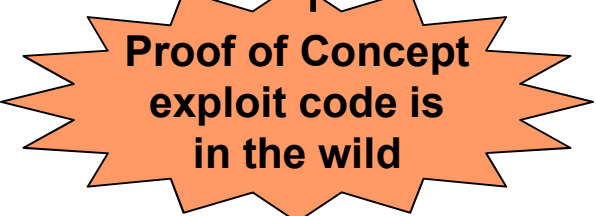
- Microsoft has one recommended workaround
 - Use a firewall to block incoming TCP protocol network traffic on port 53 destined for affected Windows Server systems using the SMTP component, even if Exchange server is not installed
 - Use a firewall to block TCP protocol network traffic on port 53
 - Do not block UDP traffic on port 53 or the server will be unable to make any DNS queries to resolve domain names
- This workaround will reduce the functionality of the computer
- Additional details are in the Microsoft bulletin

What is MS04-036?

- A bulletin from Microsoft concerning a vulnerability within the Network News Transfer Protocol (NNTP) component of several operating systems
 - Exchange 2000 servers and systems that have manually enabled NNTP are primarily at risk from this vulnerability
 - Exchange 5.0 Server and Exchange 5.5 Server are not affected by this vulnerability
 - An attacker could exploit the vulnerability by constructing a malicious request that could potentially allow remote code execution
 - An attacker who successfully exploited this vulnerability could take complete control of an affected system
- Workarounds are available

What happens if I do nothing?

- This vulnerability could potentially affect systems that do not use NNTP
 - Some programs require that the NNTP component be enabled before you can install them
- An attacker could exploit the vulnerability by sending a specially crafted message to an affected system, which could then cause the affected system to execute code
 - An attacker could also access the affected component through other vectors
 - An attacker could log on to the system interactively or by using another program that passes parameters to the vulnerable component (locally or remotely)
- There is a low to medium probability that an Internet worm might result from exploitation of this vulnerability



**Proof of Concept
exploit code is
in the wild**



• Remote Code Execution

What systems are affected?

Affected systems:

- Microsoft Windows NT Server 4.0 Service Pack 6a
- Microsoft Windows 2000 Server Service Pack 3 and Microsoft Windows 2000 Server Service Pack 4
- Microsoft Windows Server™ 2003
- Microsoft Windows Server 2003 64-Bit Edition
- Microsoft Exchange 2000 Server Service Pack 3 (Uses the Windows 2000 NNTP component)
- Microsoft Exchange Server 2003 and Microsoft Exchange Server 2003 Service Pack 1 (Uses the Windows 2000 or Windows Server 2003 NNTP component)

(continued on next slide)

What systems are affected? (2)

Systems NOT affected

- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
- Microsoft Windows 2000 Professional Service Pack 3 and Microsoft Windows 2000 Professional Service Pack 4
- Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2
- Microsoft Windows XP 64-Bit Edition Service Pack 1
- Microsoft Windows XP 64-Bit Edition Version 2003
- Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)
- Microsoft Exchange Server 5.0 Service Pack 2
- Microsoft Exchange Server 5.5 Service Pack 4

What can I do about it?

- The best solution is to download the proper update (patch) from Microsoft and install it
- There are some mitigating factors that limit the impact of this issue
 - Windows NT Server 4.0, Windows 2000 Server, and Windows Server 2003 are at a reduced risk from this vulnerability because NNTP is not installed by default
 - Exchange Server 2003 disables NNTP by default
 - Manually disabling NNTP after installing Exchange Server 2000 makes the system not vulnerable to this issue

If I cannot patch, what other workarounds can I do?

- Microsoft recommends two workarounds:
 - Block the following at the firewall:
 - UDP ports 119 and 563, and TCP ports 119 and 563
 - All unsolicited inbound traffic from the Internet to help prevent attacks that may use other ports
 - Remove or disable NNTP via the Control Panel
- NNTP is a required component for Exchange 2000 Server and Exchange Server 2003
 - While NNTP may not be removed on Exchange servers, it can be disabled (NNTP is disabled by default on Exchange 2003)
- Each of these workarounds will reduce the functionality of the computer
- Additional details are in the Microsoft bulletin

What is MS04-037?

- A bulletin from Microsoft concerning vulnerabilities in the way that the Windows Shell starts applications and the way that the Program Group Converter handles specially crafted requests
 - An attacker could exploit the vulnerability if a user visited a malicious Web site or opens a malicious file attachment
 - If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system
 - User interaction is required to exploit this vulnerability
- Workarounds are available

What happens if I do nothing?

- To exploit these vulnerabilities, an attacker would have to host a malicious Web site and then persuade a user to view that Web site
 - An attacker could also create an e-mail message that has a specially crafted link, and then persuade a user to view the e-mail message and then click the malicious link
 - An attacker could also send a specially crafted .grp file to a user, and then persuade the user to open the file
- Workstations and terminal servers are primarily at risk
 - Servers are only at risk if users are given the ability to log on and to run programs

What systems are affected?

Affected systems:

- Microsoft Windows NT Server 4.0 Service Pack 6a
- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
- Microsoft Windows 2000 SP3 and Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP and Microsoft Windows XP Service Pack 1
- Microsoft Windows XP 64-Bit Edition Service Pack 1
- Microsoft Windows XP 64-Bit Edition Version 2003
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 64-Bit Edition
- Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

Systems NOT affected

- Microsoft Windows XP Service Pack 2



What can I do about it?

- The best solution is to download the proper update (patch) from Microsoft and install it
- There are some mitigating factors that limit the impact of these issues
 - In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to exploit this vulnerability
 - An attacker would have no way to force users to visit a malicious Web site
 - By default, Outlook Express 6, Outlook 2002, and Outlook 2003 open HTML e-mail messages in the Restricted sites zone
 - Outlook 98 and Outlook 2000 open HTML e-mail messages in the Restricted sites zone if the Outlook E-mail Security Update has been installed

If I cannot patch, what other workarounds can I do?

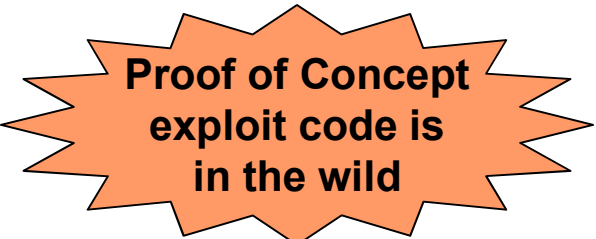
- Microsoft has tested these workarounds:
 - Install Outlook E-mail Security Update if you are using Outlook 2000 SP1 or earlier
 - Read e-mail messages in plain text format if you are using Outlook 2002 or later
 - Remove the association between .grp files and the grpconv.exe application
 - Do not open or save .grp files that you receive from untrusted sources
- Each of these workarounds will reduce the functionality of the computer
- Additional details are in the Microsoft bulletin

What is MS04-038?


- A bulletin from Microsoft concerning eight vulnerabilities in Internet Explorer 5 and 6
 - CSS heap memory corruption – remote code execution
 - Cross-domain security model – remote code execution
 - Install engine – remote code execution
 - Drag and drop events – privilege escalation
 - Double-byte address bar spoofing
 - Plug-in navigation address bar spoofing
 - Scripts in image tag files – privilege escalation
 - SSL caching – information disclosure and spoofing
- Workarounds are available for all but one of these issues

What happens if I do nothing?

- If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including
 - Installing programs
 - Viewing, changing, or deleting data
 - Creating new accounts that have full privileges
- Any systems where e-mail is read or where Internet Explorer is used frequently, such as users' workstations or terminal servers, are at the most risk from this vulnerability



**Proof of Concept
exploit code is
in the wild**

- 
- **Remote Code Execution**
 - **Local Privilege Escalation**
 - **Information Disclosure**
 - **Spoofing**



What systems are affected?

Affected systems:

- Microsoft Windows NT Server 4.0 Service Pack 6a
- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
- Microsoft Windows 2000 SP3 and Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP and Microsoft Windows XP Service Pack 1
- Microsoft Windows XP 64-Bit Edition Service Pack 1
- Microsoft Windows XP 64-Bit Edition Version 2003
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 64-Bit Edition
- Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

(continued on next slide)



What systems are affected? (2)

Affected components:

- Internet Explorer 5.01 Service Pack 3 on Windows 2000 SP3
- Internet Explorer 5.01 Service Pack 4 on Windows 2000 SP4
- Internet Explorer 5.5 Service Pack 2 on Microsoft Windows Me
- Internet Explorer 6 on Windows XP
- Internet Explorer 6 Service Pack 1 on Microsoft Windows 2000 Service Pack 3, on Microsoft Windows 2000 Service Pack 4, on Microsoft Windows XP, or on Microsoft Windows XP Service Pack 1
- Internet Explorer 6 Service Pack 1 on Microsoft Windows NT Server 4.0 Service Pack 6a, on Microsoft Windows NT Server 4.0 Terminal Service Edition Service Pack 6, on Microsoft Windows 98, on Microsoft Windows 98 SE, or on Microsoft Windows Me
- Internet Explorer 6 for Windows XP Service Pack 1 (64-Bit Edition)
- Internet Explorer 6 for Windows Server 2003
- Internet Explorer 6 for Windows Server 2003 64-Bit Edition and Windows XP 64-Bit Edition Version 2003
- Internet Explorer 6 for Windows XP Service Pack 2



What can I do about it?

- The best solution is to download the proper update (patch) from Microsoft and install it
- There are some mitigating factors that limit the impact of one or more of these issues
 - An attacker would have to host a Web site that contains a Web page that is used to exploit this vulnerability
 - An attacker would have no way to force users to visit a malicious Web site
 - By default, Outlook Express 6, Outlook 2002, and Outlook 2003 open HTML e-mail messages in the Restricted sites zone
 - Outlook 98 and Outlook 2000 open HTML e-mail messages in the Restricted sites zone if the Outlook E-mail Security Update has been installed
 - Before the user visits a legitimate SSL protected Web site, an attacker would have to redirect the user's navigation from the legitimate Web site to their malicious Web site that has the same host name

If I cannot patch, what other workarounds can I do?

- Microsoft has tested these workarounds:
 - Prompt before running ActiveX controls and active scripting in the Internet zone and in the Intranet zone
 - Restrict Web sites to only your trusted Web sites
 - Install Outlook E-mail Security Update if you are using Outlook 2000 SP1 or earlier
 - If you are using Outlook 2002 or Outlook Express 6.0 SP1 or later, read e-mail messages in plain text format to help protect yourself from the HTML e-mail attack vector
- Each of these workarounds will reduce the functionality of the computer
- Additional details are in the Microsoft bulletin

Where do I get more information?

- The October 2004 bulletins are available from Microsoft at:

http://www.microsoft.com/security/bulletins/200410_windows.msp

http://www.microsoft.com/security/bulletins/200410_office.msp

- Details on updating specific operating systems are available from Microsoft at:

<http://www.microsoft.com/security/protect/default.asp>

- Details on Microsoft's severity rating system are available at:

<http://go.microsoft.com/fwlink/?LinkId=21140>



An Invitation to Participate

- The Storm Center's success is based on the active participation of thousands of users
- All Internet users, information analysis and sharing centers, and others willing to participate in a large distributed data collection and analysis project are invited to join
- Details are online at <http://isc.sans.org>

