



Summary of Critical Patches – September 2007

Microsoft Security Bulletin - MS07-051

Vulnerability in Microsoft Agent

MS07-051 Vulnerability in Microsoft Agent Could Allow Remote Code Execution

Affected Software

Microsoft Windows 2000 Service Pack 4

Vulnerability

An input validation failure allows remote code execution via crafted URLs with the rights of the logged on user.

Vulnerability Information

This critical security update resolves a privately reported vulnerability. A remote code execution vulnerability exists in the Microsoft Agent Active-X control in the way that it handles certain specially crafted URLs. The vulnerability could allow an attacker to remotely execute code on the affected system.

Microsoft Agent is a component of the Microsoft Windows operating system that uses interactive animated characters to guide users and can make learning to use a computer easier.

Comment / Mitigation:

- 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. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit a malicious Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's Web site.
- An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Microsoft Monthly Patch Summary - Date: 12th September 2007

- The Restricted sites zone helps reduce attacks that could try to exploit this vulnerability by preventing ActiveX controls from being used when reading HTML e-mail messages. However, if a user clicks a link in an e-mail message, they could still be vulnerable to this issue through the Web-based attack scenario.
- By default, all supported versions of Microsoft Outlook and Microsoft Outlook Express open HTML e-mail messages in the Restricted sites zone. The Restricted sites zone helps reduce attacks that could try to exploit this vulnerability by preventing Active Scripting and ActiveX controls from being used when reading HTML e-mail. However, if a user clicks on a link within an e-mail they could still be vulnerable to this issue through the Web-based attack scenario.

You can help prevent attempts to instantiate this ActiveX control in Internet Explorer by setting the kill bit for the control in the registry. For instruction see:

<http://www.microsoft.com/technet/security/Bulletin/MS07-051.msp>

References:

<http://www.microsoft.com/technet/security/Bulletin/MS07-051.msp>

<http://isc.sans.org/>

Summary of Important Patches

Microsoft Security Bulletin - MS07-052

Vulnerability in Crystal Reports for Visual Studio

MS07-052 Vulnerability in Crystal Reports for Visual Studio Could Allow Remote Code Execution

Affected Software

Visual Studio .NET 2002 Service Pack 1
Visual Studio .NET 2003
Visual Studio .NET 2003 Service Pack 1
Visual Studio 2005
Visual Studio 2005 Service Pack 1

Vulnerability

Input validation failure leads to a buffer overflow that allows remote code execution via a crafted Crystal Reports "RPT" file with the rights of the logged on user.

Vulnerability Information

This security update resolves a publicly disclosed vulnerability. This vulnerability could allow remote code execution if a user opens a specially crafted RPT file.

This is an important security update for supported editions of Visual Studio that include a custom version of Crystal Reports. Only the specific editions of Visual Studio listed in the affected Software section are affected because they contain Crystal Reports.

This security update addresses the vulnerability by modifying the way that Crystal Reports for Visual Studio handles RPT files.

Comment:

An attacker could exploit the vulnerability by sending an affected user a malformed RPT file as an e-mail attachment, or hosting the file on a malicious or compromised Web site.

An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

References:

<http://www.microsoft.com/technet/security/Bulletin/MS07-052.msp>
<http://isc.sans.org/>

Microsoft Security Bulletin - MS07-053

Vulnerability in Windows Services for UNIX

MS07-053 Vulnerability in Windows Services for UNIX Could Allow Elevation of Privilege

Affected Software

Windows 2000 Service Pack 4
Windows XP Service Pack 2
Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2
Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2
Window Vista
Windows Vista x64 Edition

Vulnerability

SUID binaries allow escalation of privileges.

Vulnerability Information

This security update resolves a vulnerability existing in Windows Services for UNIX 3.0, Windows Services for UNIX 3.5, and Subsystem for UNIX-based Applications where running certain SETUID (set-user-identifier-on-execution) binary files could allow an attacker to gain elevation of privilege.

Users of client computers can set the SETUID bit for a file. An executable file which has the SETUID bit set will execute under the user ID of the file's owner, not the user ID of the user who is executing the file.

This is an important security update for supported releases of Windows 2000, Windows Server 2003, Windows Services for UNIX 3.0, Windows Services for UNIX 3.5, and Subsystem for UNIX-based Applications, a component of Windows Server 2003 and Windows Vista.

Comment:

An attacker who successfully exploited this vulnerability could gain elevation of privilege on an affected system. Users whose accounts are configured to have fewer user rights on the guest operating system are **not** less impacted than users who operate with administrative user rights on the guest operating system. However an attacker would have to log on locally to an affected system and run certain SETUID binary files.

References:

<http://www.microsoft.com/technet/security/Bulletin/MS07-053.msp>
<http://isc.sans.org/>

Microsoft Security Bulletin - MS07-054

Vulnerability in MSN Messenger and Windows Live Messenger

MS07-054 Vulnerability in MSN Messenger and Windows Live Messenger Could Allow Remote Code Execution

Affected Software

Microsoft Windows 2000 Service Pack 4	MSN Messenger 6.2 MSN Messenger 7.0
Windows XP Service Pack 2	MSN Messenger 6.2 MSN Messenger 7.0 MSN Messenger 7.5 Windows Live Messenger 8.0
Windows XP Professional x64 Edition	MSN Messenger 6.2 MSN Messenger 7.0 MSN Messenger 7.5 Windows Live Messenger 8.0
Windows XP Professional x64 Edition Service Pack 2	MSN Messenger 6.2 MSN Messenger 7.0 MSN Messenger 7.5 Windows Live Messenger 8.0
Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2	MSN Messenger 6.2 MSN Messenger 7.0 MSN Messenger 7.5 Windows Live Messenger 8.0
Windows Server 2003 x64 Edition	MSN Messenger 6.2 MSN Messenger 7.0 MSN Messenger 7.5 Windows Live Messenger 8.0
Windows Server 2003 x64 Edition Service Pack 2	MSN Messenger 6.2 MSN Messenger 7.0 MSN Messenger 7.5 Windows Live Messenger 8.0
Windows Vista	MSN Messenger 6.2 MSN Messenger 7.0 MSN Messenger 7.5 Windows Live Messenger 8.0
Windows Vista x64 Edition	MSN Messenger 6.2 MSN Messenger 7.0 MSN Messenger 7.5 Windows Live Messenger 8.0

Vulnerability

Unspecified failure allows remote code execution with the rights of the logged on user.

Vulnerability Information

A remote code execution vulnerability exists in MSN Messenger 6.2, 7.0, 7.5, and Windows Live Messenger 8.0. The vulnerability could allow remote code execution when a user chooses to accept a webcam or video chat invitation from an attacker. An attacker who successfully exploited this vulnerability could take complete control of the affected system.

The vulnerability exists due to the way MSN Messenger or Windows Live Messenger handles specially crafted webcam or video chat sessions. As a result, memory may be corrupted in such a way that an attacker could execute arbitrary code in the security context of the logged-in user.

Comment / mitigation:

To exploit the vulnerability, an attacker would have to persuade a user to accept a webcam or video chat invitation in an MSN Messenger or Windows Live Messenger message. An attacker would have no way to force users to accept the webcam or video chat invitation. Instead, an attacker would have to convince users to accept the webcam or video chat invitation.

An attacker who successfully exploited this vulnerability could gain the same user rights as the local user.

Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Users of Windows Live Messenger 8.1, released in January 2007, are already protected from this vulnerability. Users of MSN Messenger 7.0.0820, recently released, are also already protected from this vulnerability.

References:

<http://www.microsoft.com/technet/security/Bulletin/MS07-054.msp>

<http://isc.sans.org/>