

Alert: Microsoft Security Bulletin MS05-020 – Cumulative Security Update for Internet Explorer (890923)

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2005-04/0030.html>

From: Russ Cooper (*Russ.Cooper_at_TRUSECURE.CA*)

Date: 04/12/05

Date: Tue, 12 Apr 2005 14:33:31 -0400

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Microsoft Security Bulletin MS05-020:
Cumulative Security Update for Internet Explorer (890923)

Bulletin URL:

<<http://www.microsoft.com/technet/security/Bulletin/MS05-020.mspx>>

Version Number: 1.0

Issued Date: Tuesday, April 12, 2005

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Critical

Patch(es) Replaced: This update replaces the update that is included with Microsoft Security Bulletin MS05-014. That update is also a cumulative update.

Caveats: Microsoft Knowledge Base Article 890923 documents the currently known issues that customers may experience when they install this security update. The article also documents recommended solutions for these issues. For more information, see Microsoft Knowledge Base Article 890923. This update does include hotfixes that have been released since the release of MS04-004 or MS04-025 but they will only be installed on systems that need them. Customers who have received hotfixes from Microsoft or from their support providers since the release of MS04-004 or MS04-025 should review the FAQ 'I have received a hotfix from Microsoft or my support provider since the release of MS04-004. Is that hotfix included in this security update?' in the FAQ section for this update to determine how to ensure that the necessary hotfixes are installed. Microsoft Knowledge Base Article 890923 also documents this in more detail.

Tested Software:

Affected Software:

- * Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000 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 (Itanium)
- * Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium)
- * Microsoft Windows Server 2003
- * Microsoft Windows Server 2003 for Itanium-based Systems
- * Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME) Tested Microsoft Windows Components:
- * Internet Explorer 6 for Windows Server 2003 (all versions) and for Windows XP 64-Bit Edition, Version

Alert: Microsoft Security Bulletin MS05-020 – Cumulative Security Update for Internet Explorer (890923)

2003

Affected Components:

-
- * Internet Explorer 5.01 Service Pack 3 on Microsoft Windows 2000 Service Pack 3:
<<http://tinyurl.com/5juub>>
 - * Internet Explorer 5.01 Service Pack 4 on Microsoft Windows 2000 Service Pack 4: Internet Explorer 5.5 Service Pack 2 on Microsoft Windows Millennium Edition – Review the FAQ section of this bulletin for details about this version.
<<http://tinyurl.com/6g3qc>>
 - * Internet Explorer 6 Service Pack 1 on Microsoft Windows 2000 Service Pack 3, on Microsoft Windows 2000 Service Pack 4, or on Microsoft Windows XP Service Pack 1: Internet Explorer 6 Service Pack 1 on Microsoft Windows 98, on Microsoft Windows 98 SE, or on Microsoft Windows Millennium Edition – Review the FAQ section of this bulletin for details about this version.
<<http://tinyurl.com/6yhbs>>
 - * Internet Explorer 6 Service Pack 1 for Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium):
<<http://tinyurl.com/6un7t>>
 - * Internet Explorer 6 for Microsoft Windows Server 2003:
<<http://tinyurl.com/3nuqd>>
 - * Internet Explorer 6 for Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium):
<<http://tinyurl.com/4k3me>>
 - * Internet Explorer 6 for Microsoft Windows XP Service Pack 2:
<<http://tinyurl.com/6cfeg>>

Technical Description:

-
- * DHTML Object Memory Corruption Vulnerability – CAN-2005-0553 A remote code execution vulnerability exists in Internet Explorer because of the way that it handles certain DHTML objects. An attacker could exploit the vulnerability by constructing a malicious Web page. This malicious Web page could 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.
 - * URL Parsing Memory Corruption Vulnerability – CAN-2005-0554 A remote code execution vulnerability exists in Internet Explorer because of the way that it handles certain URLs. An attacker could exploit the vulnerability by constructing a malicious Web page. This malicious Web page 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.
 - * Content Advisor Memory Corruption Vulnerability – CAN-2005-0555 A remote code execution vulnerability exists in Internet Explorer because of the way that it handles Content Advisor files. An attacker could exploit the vulnerability by constructing a specially crafted Content Advisor file. This malicious Content Advisor file could potentially allow remote code execution if a user visited a malicious Web site or viewed a malicious e-mail message and accepted the installation of the file. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, significant user interaction is required to exploit this vulnerability.

This email is sent to NTBugtraq automatically as a service to my subscribers. (v4.01.1928.12470)

Cheers,
Russ Cooper – Senior Scientist – Cybertrust/NTBugtraq Editor

NT-Bugtraq: Alert: Microsoft Security Bulletin MS05-020 – Cumulative Security Update for Internet Explorer (890923)

--

NTBugtraq Editor's Note:

Most viruses these days use spoofed email addresses. As such, using an Anti-Virus product which a

--

Alert: Microsoft Security Bulletin MS05-020 – Cumulative Security Update for Internet Explorer (890923)