

Network Box February 2010 Report on Microsoft Patch Tuesday

Target Audience: Network Box Customers using all versions of Microsoft Windows

Prepared by: Network Box Security Response

Dated: 9th February 2010

February 2010 Executive Summary

This month, Microsoft releases thirteen security bulletins covering twenty six vulnerabilities. Of these, Network Box Security Response would like to draw your attention to these in particular:

- MS10-006 affecting the SMB Client
- MS10-007 affecting the Windows Shell Handler (for both mail and web)
- MS10-008 affecting the Internet Explorer ActiveX Kill Bits
- MS10-013 affecting the Microsoft DirectShow system

These issues affect a large number of versions of Microsoft Windows and Office applications. Most are remotely exploitable.

As well as our ongoing Anti-Virus protection updates (primarily targeting known exploits), Network Box Security Response is also pro-actively releasing a number of IDPS signatures to defend against the vulnerabilities themselves, where possible.

To provide the best and fullest protection, we, of course, recommend all customers apply the Microsoft updates and patch as soon as possible.

Network Box Corporation has joined the Microsoft Active Protections Program (MAPP), and is provided with vulnerability information in advance of Microsoft's monthly security update release to offer protections to customers efficiently and effectively. By receiving vulnerability information earlier, our customers benefit from additional possible improvements that provide security protection such as IPS and Anti-Virus. The protection technologies released this month are a result of this MAPP partnership between Microsoft and Network Box.

MS 10-003

Bulletin ID	CVE ID	Exploitability	Network Box	Notes
MS 10-003	CVE-2010-0243	1 (Consistent exploit code likely)	Partial, A/V	Urgent Patch

Vulnerability in Microsoft Office (MSO) Could Allow Remote Code Execution

This security update resolves a privately reported vulnerability in Microsoft Office that could allow remote code execution if a user opens a specially crafted Office file. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

This security update is rated Important for all supported editions of Microsoft Office XP and Microsoft Office 2004 for Mac.

Severity Analysis

Microsoft classifies this as important, with an exploitability index assessment of 1 (consistent exploit code likely).

Network Box Analysis

Network Box Security Response has analysed this threat, and considers it to be complex to exploit, but critical. The protection updates released by Microsoft are effective.

Network Box Protection

Due to the complexity of this threat, it is unlikely that Network Box will be able to provide protection against all exploits of this. In co-operations with our partners, however, we are releasing anti-virus signatures to protect against known exploits.

Recommendations

We recommend that all customers operating affected Microsoft Windows systems, apply the Microsoft update.

MS 10-004

Bulletin ID	CVE ID	Exploitability	Network Box	Notes
MS 10-004	CVE-2010-0029	2 (Inconsistent exploit code likely)	Partial, AV	Patch
MS 10-004	CVE-2010-0030	1 (Consistent exploit code likely)	Partial, AV	Urgent Patch
MS 10-004	CVE-2010-0031	1 (Consistent exploit code likely)	Partial, AV	Urgent Patch
MS 10-004	CVE-2010-0032	1 (Consistent exploit code likely)	Partial, AV	Urgent Patch
MS 10-004	CVE-2010-0033	1 (Consistent exploit code likely)	Partial, AV	Urgent Patch
MS 10-004	CVE-2010-0034	1 (Consistent exploit code likely)	Partial, AV	Urgent Patch

Vulnerability in Microsoft Office PowerPoint could allow Remote Code Execution

This security update resolves six privately reported vulnerabilities in Microsoft Office PowerPoint. The vulnerabilities could allow remote code execution if a user opens a specially crafted PowerPoint file. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

This security update is rated Important for supported editions of Microsoft Office PowerPoint 2002 and Microsoft Office PowerPoint 2003, and Microsoft Office 2004 for Mac.

Severity Analysis

Microsoft classifies these as important, with a maximum exploitability index assessment of 1 (consistent exploit code likely).

Network Box Analysis

Network Box Security Response has analysed these threats, and considers them to be complex to exploit, but critical. The protection updates released by Microsoft are effective.

Network Box Protection

Due to the complexity of these threats, it is unlikely that Network Box will be able to provide protection against all exploits of these. In co-operations with our partners, however, we are releasing anti-virus signatures to protect against known exploits.

Recommendations

We recommend that all customers operating affected Microsoft Windows systems, apply the Microsoft update.

MS 10-005

Bulletin ID	CVE ID	Exploitability	Network Box	Notes
MS 10-005	CVE-2010-0028	2 (Inconsistent exploit code likely)	Partial, AV	Patch

Vulnerability in Microsoft Paint Could Allow Remote Code Execution

This security update resolves a privately reported vulnerability in Microsoft Paint. The vulnerability could allow remote code execution if a user viewed a specially crafted JPEG image file using Microsoft Paint. 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.

This security update is rated Moderate for Microsoft Windows 2000, Windows XP, and Windows Server 2003.

Severity Analysis

Microsoft classifies this as moderate, with an exploitability index assessment of 2 (inconsistent exploit code likely).

Network Box Analysis

Network Box Security Response has analysed this threat, and considers it to be complex to exploit, and moderately impacting. The protection updates released by Microsoft are effective.

Network Box Protection

Due to the complexity of this threat, it is unlikely that Network Box will be able to provide protection against all exploits of this. In co-operations with our partners, however, we are releasing anti-virus signatures to protect against known exploits.

Recommendations

We recommend that all customers operating affected Microsoft Windows systems, apply the Microsoft update.

MS 10-006

Bulletin ID	CVE ID	Exploitability	Network Box	Notes
MS 10-006	CVE-2010-0016	2 (Inconsistent exploit code likely)	IPS-1-300000030	Patch
MS 10-006	CVE-2010-0017	1 (Consistent exploit code likely)	n/a	Urgent Patch

Vulnerability in SMB Client Could Allow Remote Code Execution

This security update resolves two privately reported vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if an attacker sent a specially crafted SMB response to a client-initiated SMB request. To exploit these vulnerabilities, an attacker must convince the user to initiate an SMB connection to a malicious SMB server.

This security update is rated Critical for Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows 7, and Windows Server 2008 R2, and is rated Important for Windows Vista and Windows Server 2008.

Severity Analysis

Microsoft classifies this as critical, with a maximum exploitability index assessment of 1 (consistent exploit code likely).

Network Box Analysis

Network Box Security Response has analysed these threats, and considers them to be complex to exploit, but critical. The protection updates released by Microsoft are effective.

Network Box Protection

Network Box Security Response has been releasing multiple active NBIDPS signatures (including 1-300000030) to detect and block these threats. These signatures require the new NBIDPS system - available to customers with this new system.

Recommendations

We recommend that all customers operating affected Microsoft Windows systems, apply the Microsoft update.

MS 10-007

Bulletin ID	CVE ID	Exploitability	Network Box	Notes
MS 10-007	CVE-2010-0027	1 (Consistent exploit code likely)	IPS-1-300000031	Urgent Patch

Vulnerability in Windows Shell Handler Could Allow Remote Code Execution

This security update resolves a privately reported vulnerability in Microsoft Windows 2000, Windows XP, and Windows Server 2003. Other versions of Windows are not impacted by this security update. The vulnerability could allow remote code execution if an application, such as a Web browser, passes specially crafted data to the ShellExecute API function through the Windows Shell Handler.

This security update is rated Critical for all supported editions of Microsoft Windows 2000, Windows XP, and Windows Server 2003.

Severity Analysis

Microsoft classifies this as critical, with an exploitability index assessment of 1 (consistent exploit code likely).

Network Box Analysis

Network Box Security Response has analysed this threat, and considers it to be complex to exploit, but critical. The protection updates released by Microsoft are effective.

Network Box Protection

Network Box Security Response has been releasing multiple active NBIDPS signatures (including 1-300000031) to detect and block this threat. These signatures require the new NBIDPS system - available to customers with this new system.

Recommendations

We recommend that all customers operating affected Microsoft Windows systems, apply the Microsoft update.

MS 10-008

Bulletin ID	CVE ID	Exploitability	Network Box	Notes
MS 10-008	CVE-2010-0252	1 (Consistent exploit code likely)	IPS-1-300000032	Urgent Patch

Cumulative Security Update of ActiveX Kill Bits

This security update addresses a privately reported vulnerability for Microsoft software. This security update is rated Critical for all supported editions of Microsoft Windows 2000 and Windows XP, Important for all supported editions of Windows Vista and Windows 7, Moderate for all supported editions of Windows Server 2003, and Low for all supported editions of Windows Server 2008 and Windows Server 2008 R2.

The vulnerability could allow remote code execution if a user views a specially crafted Web page that instantiates an ActiveX control with Internet Explorer. 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. This update also includes kill bits for four third-party ActiveX controls.

The security update addresses the vulnerability by setting a kill bit so that the vulnerable control does not run in Internet Explorer.

Severity Analysis

Microsoft classifies this as critical, with an exploitability index assessment of 1 (consistent exploit code likely).

Network Box Analysis

Network Box Security Response has analysed this threat, and considers it to be complex to exploit, but critical. The protection updates released by Microsoft are effective.

Network Box Protection

Network Box Security Response has been releasing multiple active NBIDPS signatures (including 1-300000032) to detect and block this threat. These signatures require the new NBIDPS system - available to customers with this new system.

Recommendations

We recommend that all customers operating affected Microsoft Windows systems, apply the Microsoft update.

MS 10-009

Bulletin ID	CVE ID	Exploitability	Network Box	Notes
MS 10-009	CVE-2010-0239	2 (Inconsistent exploit code likely)	n/a	Patch
MS 10-009	CVE-2010-0240	2 (Inconsistent exploit code likely)	n/a	Patch
MS 10-009	CVE-2010-0241	2 (Inconsistent exploit code likely)	n/a	Patch
MS 10-009	CVE-2010-0242	3 (Functioning exploit code unlikely)	n/a	Patch

Vulnerability in Windows TCP/IP Could Allow Remote Code Execution

This security update resolves four privately reported vulnerabilities in Microsoft Windows. The most severe of these vulnerabilities could allow remote code execution if specially crafted packets are sent to a computer with IPv6 enabled. An attacker could try to exploit the vulnerability by creating specially crafted ICMPv6 packets and sending the packets to a system with IPv6 enabled. This vulnerability may only be exploited if the attacker is on-link.

This security update is rated Critical for Windows Vista and Windows Server 2008.

The security update addresses the vulnerabilities by changing the way Windows TCP/IP performs bounds checking and other packet handling operations.

Severity Analysis

Microsoft classifies these as critical, with a maximum exploitability index assessment of 2 (inconsistent exploit code likely).

Network Box Analysis

Network Box Security Response has analysed these threats, and considers them to be complex to exploit, but critical. The protection updates released by Microsoft are effective.

Network Box Protection

Due to the complexity of these threats, and the limitation of impact to those using the currently rare IPv6 protocol, it is unlikely that Network Box will be able to provide protection against all exploits of these.

Recommendations

We recommend that all customers operating affected Microsoft Windows systems, apply the Microsoft update.

MS 10-010

Bulletin ID	CVE ID	Exploitability	Network Box	Notes
MS 10-010	CVE-2010-0026	3 (Functioning exploit code unlikely)	Partial, A/V	Patch

Vulnerability in Windows Hyper-V Could Allow Denial of Service

This security update resolves a privately reported vulnerability in Windows Server 2008 Hyper-V and Windows Server 2008 R2 Hyper-V. The vulnerability could allow denial of service if a malformed sequence of machine instructions is run by an authenticated user in one of the guest virtual machines hosted by the Hyper-V server. An attacker must have valid logon credentials and be able to log on locally into a guest virtual machine to exploit this vulnerability. The vulnerability could not be exploited remotely or by anonymous users.

This security update is rated Important for all supported x64-based editions of Windows Server 2008 and Windows Server 2008 R2.

The security update addresses the vulnerability by correcting the way Hyper-V server validates encoding on machine instructions executed inside its guest virtual machines.

Severity Analysis

Microsoft classifies this as important, with an exploitability index assessment of 3 (functioning exploit code unlikely).

Network Box Analysis

Network Box Security Response has analysed this threat, and considers it to be complex to exploit, but important. The protection updates released by Microsoft are effective.

Network Box Protection

Due to the complexity of this threat, it is unlikely that Network Box will be able to provide protection against all exploits of this. In co-operations with our partners, however, we are releasing anti-virus signatures to protect against known exploits.

Recommendations

We recommend that all customers operating affected Microsoft Windows systems, apply the Microsoft update.

MS 10-011

Bulletin ID	CVE ID	Exploitability	Network Box	Notes
MS 10-011	CVE-2010-0023	1 (Consistent exploit code likely)	Partial, A/V	Urgent Patch

Vulnerability in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege

This security update resolves a privately reported vulnerability in Microsoft Windows Client/Server Run-time Subsystem (CSRSS) in Microsoft Windows 2000, Windows XP, and Windows Server 2003. Other versions of Windows are not affected. The vulnerability could allow elevation of privilege if an attacker logs on to the system and starts a specially crafted application designed to continue running after the attacker logs out. An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability. The vulnerability could not be exploited by anonymous users.

This security update is rated Important for all supported editions of Microsoft Windows 2000, Windows XP, and Windows Server 2003.

The security update addresses the vulnerability by correcting the manner in which users' processes are terminated upon logout.

Severity Analysis

Microsoft classifies this as important, with an exploitability index assessment of 1 (consistent exploit code likely).

Network Box Analysis

Network Box Security Response has analysed this threat, and considers it to be complex to exploit, but important. The protection updates released by Microsoft are effective.

Network Box Protection

Due to the complexity of this threat, it is unlikely that Network Box will be able to provide protection against all exploits of this. In co-operations with our partners, however, we are releasing anti-virus signatures to protect against known exploits.

Recommendations

We recommend that all customers operating affected Microsoft Windows systems, apply the Microsoft update.

MS 10-012

Bulletin ID	CVE ID	Exploitability	Network Box	Notes
MS 10-012	CVE-2010-0020	2 (Inconsistent exploit code likely)	IPS-1-300000033	Patch
MS 10-012	CVE-2010-0021	2 (Inconsistent exploit code likely)	n/a	Patch
MS 10-012	CVE-2010-0022	3 (Functioning exploit code unlikely)	IPS-1-300000034	Patch
MS 10-012	CVE-2010-0231	1 (Consistent exploit code likely)	n/a	Urgent Patch

Vulnerability in SMB Server Could Allow Remote Code Execution

This security update resolves several privately reported vulnerabilities in Microsoft Windows. The most severe of these vulnerabilities could allow remote code execution if an attacker created a specially crafted SMB packet and sent the packet to an affected system. Firewall best practices and standard default firewall configurations can help protect networks from attacks originating outside the enterprise perimeter that would attempt to exploit these vulnerabilities.

This security update is rated Important for all supported editions of Microsoft Windows.

The security update addresses these vulnerabilities by correcting the way that SMB validates SMB requests.

Severity Analysis

Microsoft classifies these as important, with a maximum exploitability index assessment of 1 (consistent exploit code likely).

Network Box Analysis

Network Box Security Response has analysed these threats, and considers them to be complex to exploit, but important. The protection updates released by Microsoft are effective.

Network Box Protection

Network Box Security Response has been releasing multiple active NBIDPS signatures (including 1-300000033 and 1-300000034) to detect and block these threats. These signatures require the new NBIDPS system - available to customers with this new system.

Recommendations

We recommend that all customers operating affected Microsoft Windows systems, apply the Microsoft update.

MS 10-013

Bulletin ID	CVE ID	Exploitability	Network Box	Notes
MS 10-013	CVE-2010-0250	1 (Consistent exploit code likely)	Partial, AV	Urgent Patch

Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution

This security update resolves a privately reported vulnerability in Microsoft DirectShow. The vulnerability could allow remote code execution if a user opened a specially crafted AVI file. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

This security update is rated Critical for all supported editions of Microsoft Windows except for all supported Itanium-based editions of Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2, for which this security update is rated Important.

The security update addresses the vulnerability by correcting the way that DirectShow opens AVI files.

Severity Analysis

Microsoft classifies this as critical, with an exploitability index assessment of 1 (consistent exploit code likely).

Network Box Analysis

Network Box Security Response has analysed this threat, and considers it to be complex to exploit, but critical. The protection updates released by Microsoft are effective.

Network Box Protection

Due to the complexity of this threat, it is unlikely that Network Box will be able to provide protection against all exploits of this. In co-operations with our partners, however, we are releasing anti-virus signatures to protect against known exploits.

Recommendations

We recommend that all customers operating affected Microsoft Windows systems, apply the Microsoft update.

MS 10-014

Bulletin ID	CVE ID	Exploitability	Network Box	Notes
MS 10-014	CVE-2010-0035	3 (Functioning exploit code unlikely)	Partial, AV	Patch

Vulnerability in Kerberos Could Allow Denial of Service

This security update resolves a privately reported vulnerability in Microsoft Windows. The vulnerability could allow denial of service if a specially crafted ticket renewal request is sent to the Windows Kerberos domain from an authenticated user on a trusted non-Windows Kerberos realm. The denial of service could persist until the domain controller is restarted.

This security update is rated Important for all supported editions of Microsoft Windows 2000 Server, Windows Server 2003, and Windows Server 2008.

This update addresses the vulnerability by correcting the way the Kerberos server deals with ticket renewal requests.

Severity Analysis

Microsoft classifies this as important, with an exploitability index assessment of 3 (functioning exploit code unlikely).

Network Box Analysis

Network Box Security Response has analysed this threat, and considers it to be complex to exploit, but important. The protection updates released by Microsoft are effective.

Network Box Protection

Due to the complexity of this threat, it is unlikely that Network Box will be able to provide protection against all exploits of this. In co-operations with our partners, however, we are releasing anti-virus signatures to protect against known exploits.

Recommendations

We recommend that all customers operating affected Microsoft Windows systems, apply the Microsoft update.

MS 10-015

Bulletin ID	CVE ID	Exploitability	Network Box	Notes
MS 10-015	CVE-2010-0232	1 (Consistent exploit code likely)	Partial, A/V	Urgent Patch
MS 10-015	CVE-2010-0233	2 (Inconsistent exploit code likely)	Partial, A/V	Patch

Vulnerability in Windows Kernel could allow Elevation of Privilege

This security update resolves one publicly disclosed and one privately reported vulnerability in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logged on to the system and then ran a specially crafted application. To exploit either vulnerability, an attacker must have valid logon credentials and be able to log on locally. The vulnerabilities could not be exploited remotely or by anonymous users.

This security update is rated Important for all supported editions of Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 for 32-bit Systems.

The security update addresses the vulnerabilities by ensuring that the Windows Kernel handles exceptions properly.

Severity Analysis

Microsoft classifies these as important, with a maximum exploitability index assessment of 1 (consistent exploit code likely).

Network Box Analysis

Network Box Security Response has analysed these threats, and considers them to be complex to exploit, but critical. The protection updates released by Microsoft are effective.

Network Box Protection

Due to the complexity of these threats, it is unlikely that Network Box will be able to provide protection against all exploits of these. In co-operations with our partners, however, we are releasing anti-virus signatures to protect against known exploits.

Recommendations

We recommend that all customers operating affected Microsoft Windows systems, apply the Microsoft update.