

Network Box January 21st 2010 Supplemental Report on Microsoft Patch Tuesday

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

Prepared by: Network Box Security Response

Dated: 21st January 2010

21st January 2010 Supplemental Executive Summary

In response to highly publicised attacks reportedly exploiting a zero-day (without protection) vulnerability in the Microsoft Internet Explorer web browser, Microsoft has released, out-of-band, security bulletin MS10-002 addressing seven privately reported vulnerabilities and one publicly disclosed vulnerability in Internet Explorer.

This bulletin is:

- MS10-002 affecting Microsoft Internet Explorer and other applications using the mshtml.dll component.

While the publicised issue so far only affects Internet Explorer 6, this cumulative update also addresses seven other vulnerabilities affecting multiple versions of Internet Explorer. The updates to address these issues have now been released by Microsoft and are available for installation.

To provide the best and fullest protection, we recommend that 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 10-002

Bulletin ID	CVE ID	Exploitability	Network Box	Notes
MS 10-002	CVE-2009-4074	1 (consistent exploit code likely)	Partial, AV	Urgent Patch
MS 10-002	CVE-2010-0027	1 (consistent exploit code likely)	Partial, AV	Urgent Patch
MS 10-002	CVE-2010-0244	1 (consistent exploit code likely)	Partial, AV	Urgent Patch
MS 10-002	CVE-2010-0245	1 (consistent exploit code likely)	Partial, AV	Urgent Patch
MS 10-002	CVE-2010-0246	1 (consistent exploit code likely)	Partial, AV	Urgent Patch
MS 10-002	CVE-2010-0247	1 (consistent exploit code likely)	Partial, AV	Urgent Patch
MS 10-002	CVE-2010-0248	1 (consistent exploit code likely)	Partial, AV	Urgent Patch
MS 10-002	CVE-2010-0249	1 (consistent exploit code likely)	Partial, AV IPS-1-300000028	Urgent Patch

Cumulative Security Update for Internet Explorer

This security update resolves seven privately reported vulnerabilities and one publicly disclosed vulnerability in Internet Explorer. The more severe vulnerabilities could allow remote code execution if a user views a specially crafted Web page using 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 security update is rated Critical for all supported releases of Internet Explorer: Internet Explorer 5.01, Internet Explorer 6, Internet Explorer 6 Service Pack 1, Internet Explorer 7, and Internet Explorer 8 (except Internet Explorer 6 for supported editions of Windows Server 2003). For Internet Explorer 6 for supported editions of Windows Server 2003 as listed, this update is rated Moderate.

The security update addresses these vulnerabilities by modifying the way that Internet Explorer handles objects in memory, validates input parameters, and filters HTML attributes. For more information about the vulnerabilities see the Microsoft security bulletin.

Severity Analysis

Microsoft classifies these as critical, with a maximum exploitability index assessment of 1 (consistent exploit code likely). Microsoft Internet Explorer v6 is the most vulnerable to these problems, but security researchers have demonstrated potentially successful exploits against both Internet Explorer v7 and v8, even with DEP protection enabled.

Network Box Analysis

Network Box Security Response has analysed these threats, and considers them to be exploitable and critical. There is both general availability of public exploit code and limited targeted exploits ongoing in the wild. 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 possible exploits of this. In co-operations with our partners, however, we are releasing anti-virus signatures to protect against known exploits, and these signatures have been shown to be effective in general protection against aspects these threats (in particular, trojan dropper behavior, and script obfuscation techniques). In addition, we have released NBIDPS signature IPS-1-300000028 to protect against the most common exploit technique.

Recommendations

We recommend that all customers operating affected Microsoft Windows systems, apply the Microsoft updates as a matter of urgency.