

Network Box March 30th 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: 30th March 2010

30th March 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 MS10-018 addressing nine privately reported vulnerabilities and one publicly disclosed vulnerability in Internet Explorer.

- MS10-018 affecting Microsoft Internet Explorer

While the publicised issue so far only affects Internet Explorer v6 and v7, this cumulative update also addresses nine other vulnerabilities affecting multiple versions of Internet Explorer (including v8). 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, 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 10-018

Bulletin ID	CVE ID	Exploitability	Network Box	Notes
MS 10-018	CVE-2010-0267	3 (Functioning exploit code unlikely)	Partial, A/V	Patch
MS 10-018	CVE-2010-0488	3 (Functioning exploit code unlikely)	Partial, A/V	Patch
MS 10-018	CVE-2010-0489	2 (Inconsistent exploit code likely)	Partial, A/V	Patch
MS 10-018	CVE-2010-0490	3 (Functioning exploit code unlikely)	Partial, A/V	Patch
MS 10-018	CVE-2010-0491	1 (Consistent exploit code likely)	Partial, A/V	Urgent Patch
MS 10-018	CVE-2010-0492	1 (Consistent exploit code likely)	Partial, A/V	Urgent Patch
MS 10-018	CVE-2010-0494	1 (Consistent exploit code likely)	IPS-1-300000046	Urgent Patch
MS 10-018	CVE-2010-0805	2 (Inconsistent exploit code likely)	IPS-1-300000045	Patch
MS 10-018	CVE-2010-0806	1 (Consistent exploit code likely)	IPS-1-300000044	Urgent Patch
MS 10-018	CVE-2010-0807	1 (Consistent exploit code likely)	Partial, A/V	Urgent Patch

Cumulative Security Update for Internet Explorer

This security update resolves nine privately reported vulnerabilities and one publicly disclosed vulnerability in Internet Explorer. The most 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.

Severity Analysis

Microsoft classifies these 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

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 cooperation with our partners, however, we are releasing antivirus signatures to protect against known exploits.

Recommendations

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