

Network Box April 2011 Report on Microsoft Patch Tuesday

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

Prepared by: Network Box Security Response

Dated: 12th April 2011

April 2011 Executive Summary

This month, Microsoft releases seventeen security bulletins covering sixty four vulnerabilities. These are:

- MS11-018 Cumulative Security Update for Internet Explorer
- MS11-019 Vulnerabilities in SMB Client Could Allow Remote Code Execution
- MS11-020 Vulnerability in SMB Server Could Allow Remote Code Execution
- MS11-021 Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution
- MS11-022 Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution
- MS11-023 Vulnerabilities in Microsoft Office Could Allow Remote Code Execution
- MS11-024 Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution
- MS11-025 Vulnerability in Microsoft Foundation Class (MFC) Library Could Allow Remote Code Execution
- MS11-026 Vulnerability in MHTML Could Allow Information Disclosure
- MS11-027 Cumulative Security Update for ActiveX Kill Bits
- MS11-028 Vulnerability in .NET Framework Could Allow Remote Code Execution
- MS11-029 Vulnerability in GDI+ Could Allow Remote Code Execution
- MS11-030 Vulnerability in DNS Resolution Could Allow Remote Code Execution
- MS11-031 Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution
- MS11-032 Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution
- MS11-033 Vulnerability in WordPad Text Converters Could Allow Remote Code Execution
- MS11-034 Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege

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

Bulletin ID	CVE ID	Exploitability	Network Box	Notes
MS11-018	CVE-2011-0094	3 – Functioning exploit code unlikely	Partial, A/V	Urgent Patch
MS11-018	CVE-2011-0346	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-018	CVE-2011-1244	1 - Consistent exploit code likely	n/a	Patch
MS11-018	CVE-2011-1245	1 - Consistent exploit code likely	n/a	Patch
MS11-018	CVE-2011-1345	1 - Consistent exploit code likely	IPS-1-300000079	Urgent Patch
MS11-019	CVE-2011-0654	2 - Inconsistent exploit code likely	n/a	Patch
MS11-019	CVE-2011-0660	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-020	CVE-2011-0661	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-021	CVE-2011-0097	1 - Consistent exploit code likely	Partial, A/V	Urgent Patch
MS11-021	CVE-2011-0098	1 - Consistent exploit code likely	Partial, A/V	Urgent Patch
MS11-021	CVE-2011-0101	1 - Consistent exploit code likely	Partial, A/V	Urgent Patch
MS11-021	CVE-2011-0103	1 - Consistent exploit code likely	Partial, A/V	Patch
MS11-021	CVE-2011-0104	1 - Consistent exploit code likely	Partial, A/V	Patch
MS11-021	CVE-2011-0105	2 - Inconsistent exploit code likely	Partial, A/V	Patch
MS11-021	CVE-2011-0978	2 - Inconsistent exploit code likely	Partial, A/V	Urgent Patch
MS11-021	CVE-2011-0979	2 - Inconsistent exploit code likely	Partial, A/V	Urgent Patch
MS11-021	CVE-2011-0980	1 - Consistent exploit code likely	Partial, A/V	Urgent Patch
MS11-022	CVE-2011-0655	2 - Inconsistent exploit code likely	Partial, A/V	Patch
MS11-022	CVE-2011-0656	2 - Inconsistent exploit code likely	Partial, A/V	Patch
MS11-022	CVE-2011-0976	2 - Inconsistent exploit code likely	Partial, A/V	Urgent Patch
MS11-023	CVE-2011-0107	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-023	CVE-2011-0977	3 – Functioning exploit code unlikely	Partial, A/V	Patch
MS11-024	CVE-2010-3974	1 - Consistent exploit code likely	n/a	Patch
MS11-025	CVE-2010-3190	3 – Functioning exploit code unlikely	n/a	Urgent Patch
MS11-026	CVE-2011-0096	1 - Consistent exploit code likely	IPS-1-300000077	Patch
MS11-027	CVE-2010-0811	1 - Consistent exploit code likely	IPS-1-300000075	Urgent Patch
MS11-027	CVE-2010-3973	1 - Consistent exploit code likely	IPS-1-300000076	Urgent Patch

Bulletin ID	CVE ID	Exploitability	Network Box	Notes
MS11-027	CVE-2011-1243	1 - Consistent exploit code likely	IPS-1-300000078	Urgent Patch
MS11-028	CVE-2010-3958	2 - Inconsistent exploit code likely	n/a	Urgent Patch
MS11-029	CVE-2011-0041	2 - Inconsistent exploit code likely	Partial, A/V	Urgent Patch
MS11-030	CVE-2011-0657	3 - Functioning exploit code unlikely	n/a	Patch
MS11-031	CVE-2011-0663	2 - Inconsistent exploit code likely	n/a	Patch
MS11-032	CVE-2011-0034	1 - Consistent exploit code likely	Partial, A/V	Patch
MS11-033	CVE-2011-0028	3 - Functioning exploit code unlikely	Partial, A/V	Patch
MS11-034	CVE-2011-0662	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-0665	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-0666	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-0667	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-0670	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-0671	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-0672	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-0673	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-0674	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-0675	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-0676	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-0677	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-1225	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-1226	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-1227	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-1228	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-1229	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-1230	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-1231	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-1232	1 - Consistent exploit code likely	n/a	Urgent Patch

Bulletin ID	CVE ID	Exploitability	Network Box	Notes
MS11-034	CVE-2011-1233	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-1234	1 - Consistent exploit code likely	n/a	Patch
MS11-034	CVE-2011-1235	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-1236	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-1237	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-1238	2 - Inconsistent exploit code likely	n/a	Patch
MS11-034	CVE-2011-1239	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-1240	1 - Consistent exploit code likely	n/a	Urgent Patch
MS11-034	CVE-2011-1241	3 - Functioning exploit code unlikely	n/a	Urgent Patch
MS11-034	CVE-2011-1242	1 - Consistent exploit code likely	n/a	Urgent Patch

Notes:

1. Some signatures may require the NBIDPS system - available to customers who are running this system.
2. This month, we are providing partial AV support for several threats. Due to the complex nature of these threats it is not possible to protect against all possible exploits in all possible circumstances.