

TopResponse Threat Advisory

Release Date: June 21, 2011.

Purpose: The Corero TopResponse team informs customers that existing IPS 5500 security features provide proactive protection for the Microsoft SMB Response Parsing Vulnerability (MS11-043,CVE-2011-1268).

Corero Products: Top Layer IPS 5500 4.X and later.

Vulnerable Infrastructure: Microsoft Windows XP SP3,Microsoft Windows XP Professional x64 Edition SP2,Microsoft Windows Server 2003 SP2,Microsoft Windows Server 2003 x64 Edition SP2,Microsoft Windows Server 2003 with SP2 for Itanium-based Systems,Microsoft Windows Vista SP1 and Microsoft Windows Vista SP2,Microsoft Windows Vista x64 Edition SP1 and Microsoft Windows Vista x64 Edition SP2,Microsoft Windows Server 2008 for 32-bit Systems and Microsoft Windows Server 2008 for 32-bit Systems SP2,Microsoft Windows Server 2008 for x64-based Systems and Microsoft Windows Server 2008 for x64-based Systems SP2,Microsoft Windows Server 2008 for Itanium-based Systems and Microsoft Windows Server 2008 for Itanium-based Systems SP2,Microsoft Windows 7 for 32-bit Systems,Microsoft Windows 7 for 32-bit Systems SP1,Microsoft Windows 7 for x64-based Systems,Microsoft Windows 7 for x64-based Systems SP1,Microsoft Windows Server 2008 R2 for x64-based Systems,Microsoft Windows Server 2008 R2 for x64-based Systems SP1,Microsoft Windows Server 2008 R2 for Itanium-based Systems, Microsoft Windows Server 2008 R2 for Itanium-based Systems SP1.

Alert Type: Critical Vulnerability

Risk Assessment: Critical

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to control vulnerable systems

Advisory Impact: Prevention

Summary: The Microsoft Server Message Block (SMB) protocol v1 and v2 contains a vulnerability in the way SMB responses are parsed. The reported vulnerability could allow an attacker to execute arbitrary code on the users systems in the context of the logged-on user by sending a specially crafted SMB response. The IPS 5500 provides proactive protection for this vulnerability.

References: Use the following sources for additional information:

Additional Information	Location
Corero Support	http://www.corero.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/Bulletin/MS11-043.msp

Relevant IPS 5500 Rules: tln-005022.