

TopResponse Threat Advisory

Release Date: August 11, 2011.

Purpose: The Corero TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against known attacks targeting the Microsoft Chart Control Information Disclosure Vulnerability (MS11-066,CVE-2011-1977).

Corero Products: Top Layer IPS 5500 and later.

Vulnerable Infrastructure: Microsoft .NET Framework 4 on Windows XP SP3, Microsoft .NET Framework 4 on Windows XP Professional x64 Edition SP2, Microsoft .NET Framework 4 on Windows Server 2003 SP2, Microsoft .NET Framework 4 on Windows Server 2003 x64 Edition SP2, Microsoft .NET Framework 4 on Windows Server 2003 with SP2 for Itanium-based Systems, Microsoft .NET Framework 4 on Windows Vista SP2, Microsoft .NET Framework 4 on Windows Vista x64 Edition SP2, Microsoft .NET Framework 4 on Windows Server 2008 for 32-bit Systems SP2, Microsoft .NET Framework 4 on Windows Server 2008 for x64-based Systems SP2, Microsoft .NET Framework 4 on Windows Server 2008 for Itanium-based Systems SP2, Microsoft .NET Framework 4 on Windows 7 for 32-bit Systems and Windows 7 for 32-bit Systems SP1, Microsoft .NET Framework 4 on Windows 7 for x64-based Systems and Windows 7 for x64-based Systems SP1, Microsoft .NET Framework 4 on Windows Server 2008 R2 for x64-based Systems and Windows Server 2008 R2 for x64-based Systems SP1, Microsoft .NET Framework 4 on Windows Server 2008 R2 for Itanium-based Systems and Windows Server 2008 R2 for Itanium-based Systems SP1, and Microsoft Chart Control for Microsoft .NET Framework 3.5 SP1.

Alert Type: Critical Vulnerability

Risk Assessment: Critical

Threat Impact: Remotely exploitable vulnerability that could allow information disclosure

Advisory Impact: Prevention

Summary: Microsoft Chart controls support creating .NET pages and Windows Forms containing visually compelling charts for financial or statistical analysis. There exists a vulnerability in the Microsoft Chart routines that verify URI content. The reported vulnerability could allow a remote attacker to read any file within a web site directory by sending a specially crafted HTTP request. The IPS 5500 provides proactive protection against known attacks targeting this vulnerability.

Recommended Action: Corero recommends the following actions:

Ensure that the rule tln-102033, “EXPLT: HTTP URI Query Value Contains Directory Traversal”, is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft Chart control infrastructure. The rule is currently enabled in the “Strict Server Protection” IPS Rule Set.

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/MS11-066.msp

Relevant IPS 5500 Rules: tln-102033.