

TopResponse Threat Advisory

Release Date: September 16, 2011.

Purpose: The Corero TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against known attacks targeting the Microsoft Windows Component Insecure Library Loading Code Execution Vulnerability (MS11-071,CVE-2011-1991).

Corero Products: Top Layer IPS 5500 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 SP2,Microsoft Windows Vista x64 Edition SP2,Microsoft Windows Server 2008 for 32-bit Systems SP2,Microsoft Windows Server 2008 for x64-based Systems SP2,Microsoft Windows Server 2008 for Itanium-based Systems SP2,Microsoft Windows 7 for 32-bit Systems and Microsoft Windows 7 for 32-bit Systems SP1,Microsoft Windows 7 for x64-based Systems and Microsoft Windows 7 for x64-based Systems SP1,Microsoft Windows Server 2008 R2 for x64-based Systems and Microsoft Windows Server 2008 R2 for x64-based Systems SP1,Microsoft Windows Server 2008 R2 for Itanium-based Systems and 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: Microsoft Windows contains shared components that are vulnerable to DLL Hijacking. The reported vulnerability could allow a remote attacker to execute arbitrary code on the vulnerable infrastructure components by opening a specially crafted e-mail or visiting a specially crafted web site, which causes vulnerable systems to attempt to download a file from an external system using either the WebDAV or the Microsoft RPC protocol. The IPS 5500 provides proactive protection against known attacks targeting this vulnerability.

Recommended Action: Corero recommends the following actions:

Ensure that the rule tln-102004, “AAUPV: HTTP Method Name Matches Specified Filter”, is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft

Windows 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/MS11-073.msp

Relevant IPS 5500 Rules: tln-102004.