

TopResponse Threat Advisory

Release Date: September 14, 2011.

Purpose: The Corero TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against known attacks targeting the Microsoft Office Component Insecure Library Loading Code Execution Vulnerability (MS11-073,CVE-2011-1980).

Corero Products: Top Layer IPS 5500 and later.

Vulnerable Infrastructure: Microsoft Office 2003 SP3,Microsoft Office 2007 SP2,Microsoft Office 2010, and Microsoft Office 2010 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 Office contains a shared component that is 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 Office 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.