

TopResponse Threat Advisory

Release Date: August 10, 2011.

Purpose: The Corero TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against known attacks targeting the Microsoft Data Access Components Insecure Library Loading Code Execution Vulnerability (MS11-059,CVE-2011-1975).

Corero Products: Top Layer IPS 5500 and later.

Vulnerable Infrastructure: Microsoft Windows 7 for 32-bit Systems and Windows 7 for 32-bit Systems SP1, Microsoft Windows 7 for x64-based Systems and Windows 7 for x64-based Systems SP1,Microsoft Windows Server 2008 R2 for x64-based Systems and Windows Server 2008 R2 for x64-based Systems SP1, and Microsoft Windows Server 2008 R2 for Itanium-based Systems and 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 Data Access Components (Windows DAC) v6.0 are technologies included in Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2 to provide access to information across the enterprise. The technologies include Microsoft ActiveX Data Objects (ADO), OLE DB, and Microsoft Open Database Connectivity (ODBC). Microsoft Windows DAC are vulnerable to a DLL Hijacking vulnerability. 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: Top Layer 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 Visio 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/MS11-059.msp

Relevant IPS 5500 Rules: tln-102004.