

TopResponse Threat Advisory

Release Date: October 13, 2011.

Purpose: The Corero TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Internet Explorer OLEAuto32.dll Remote Code Execution Vulnerability (MS11-081,CVE-2011-1995).

Corero Products: Top Layer IPS 5500 E-Series and later.

Vulnerable Infrastructure: Microsoft Internet Explorer 6 for Windows XP SP3, Microsoft Internet Explorer 6 for Windows XP Professional x64 Edition SP2, Microsoft Internet Explorer 6 for Windows Server 2003 SP2, Microsoft Internet Explorer 6 for Windows Server 2003 x64 Edition SP2, Microsoft Internet Explorer 6 for Windows Server 2003 with SP2 for Itanium-based Systems, Microsoft Internet Explorer 7 for Windows XP SP3, Microsoft Internet Explorer 7 for Windows XP Professional x64 Edition SP2, Microsoft Internet Explorer 7 for Windows Server 2003 SP2, Microsoft Internet Explorer 7 for Windows Server 2003 x64 Edition SP2, Microsoft Internet Explorer 7 for Windows Server 2003 with SP2 for Itanium-based Systems, Microsoft Internet Explorer 7 in Windows Vista SP2, Microsoft Internet Explorer 7 in Windows Vista x64 Edition SP2, Microsoft Internet Explorer 7 in Windows Server 2008 for 32-bit Systems SP2 and other software versions described in the Microsoft bulletin.

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 Internet Explorer contains a vulnerability in the way an uninitialized pointer variable is processed. The reported vulnerability could allow an attacker to execute arbitrary code on the users systems in the context of the logged-on user by enticing the user to open a specially crafted web site file.

Recommended Action: Corero recommends the following actions:

Download and apply Protection Pack 2011-10-11-03 (or later) to put this new protection into place. This will put into place protection for the Microsoft Internet Explorer OLEAuto32.dll Remote Code Execution Vulnerability that will be applied to the “Recommended Client Protection” IPS Rule Set.

In order to take advantage of the protection provided in this Protection Pack, make sure the IPS rule tln-106388 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft Excel infrastructure.

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/ms11-081.msp

Relevant IPS 5500 Rules: tln-106388.

Relevant TopResponse Protection Pack(s): 2011-10-11-03.