

## 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 Sharepoint Editform Script Injection Vulnerability (MS11-074,CVE-2011-1890).

**Corero Products:** Top Layer IPS 5500 and later.

**Vulnerable Infrastructure:** Microsoft Office Groove 2007 SP2, Microsoft Sharepoint Workspace 2010 SP1, Microsoft Office Forms Server 2007 SP2, Microsoft Office Sharepoint Server 2007 SP2, Microsoft Office Sharepoint Server 2010 and 2010 SP1, Microsoft Sharepoint Service v2.0, Microsoft Sharepoint Services v3.0 SP2, Microsoft Sharepoint Foundation 2010, Microsoft Sharepoint Foundation 2010 SP1, Microsoft Office Web Apps 2010 and 2010 SP1.

**Alert Type:** Critical Vulnerability

**Risk Assessment:** Critical

**Threat Impact:** Remotely exploitable vulnerability that could allow information disclosure

**Advisory Impact:** Prevention

**Summary:** The Microsoft Sharepoint interface implements a number of forms that are used to submit user input. There exists a vulnerability in the way user input sent through the EditForm form realized by Microsoft Sharepoint is processed. The reported vulnerability could allow a remote attacker to inject a script into a user's browser by enticing the user to click on a specially crafted web link. The IPS 5500 provides proactive protection against known attacks targeting this vulnerability.

**Recommended Action:** Corero recommends the following actions:

Ensure that the rule tln-102078, "EXPLT: HTTP URI Query Value Matches Specified Filter", is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft Sharepoint infrastructure. The rule is currently enabled in the "Strict Client Protection" and "Recommended Server Protection" IPS Rule Sets.

**References:** Use the following sources for additional information:

Additional Information	Location
<b>Corero Support</b>	<a href="http://www.corero.com/support">http://www.corero.com/support</a>
<b>Microsoft Advisory</b>	<a href="http://www.microsoft.com/technet/security/Bulletin/MS11-074.msp">http://www.microsoft.com/technet/security/Bulletin/MS11-074.msp</a>

**Relevant IPS 5500 Rules:** tln-102078.