

## TopResponse Threat Advisory

**Release Date:** August 17, 2011.

**Purpose:** The Corero TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against known attacks targeting the Microsoft Remote Desktop Web Access XSS Vulnerability (MS11-061,CVE-2011-1263).

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

**Vulnerable Infrastructure:** Microsoft Windows Server 2008 R2 for x64-based Systems and Windows Server 2008 R2 for x64-based Systems SP1 excluding Server Core installation as described in the Microsoft bulletin for the vulnerability.

**Alert Type:** Critical Vulnerability

**Risk Assessment:** Critical

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

**Advisory Impact:** Prevention

**Summary:** Microsoft Remote Desktop Web Access is a role service included in the Remote Desktop Services role that enables users to connect to a remote desktop using a Web browser by connecting to the corresponding Remote Desktop Web Access service. There exists a vulnerability in the way URL parameters are handled by the Remote Desktop Web Access implementation. 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 Remote Desktop Web Access server 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/MS11-061.msp">http://www.microsoft.com/technet/security/Bulletin/MS11-061.msp</a>

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