

## TopResponse Threat Advisory

**Release Date:** October 18, 2011.

**Purpose:** The Corero TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against known attacks targeting the Microsoft Forefront Unified Access Gateway Default Reflected XSS Vulnerability (MS11-079,CVE-2011-1897).

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

**Vulnerable Infrastructure:** Microsoft Forefront Unified Access Gateway 2010, Microsoft Forefront Unified Access Gateway 2010 Update 1, Microsoft Forefront Unified Access Gateway 2010 Update 2, and Microsoft Forefront Unified Access Gateway 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 Forefront Unified Access Gateway (UAG) contains a vulnerability in the way user requests are 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-102030, "PROTO: HTTP URI Query Name Contains Invalid Character", is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft Forefront Unified Access Gateway infrastructure. The rule is currently enabled in the "Strict Server Protection" IPS Rule Set.

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

<b>Additional Information</b>	<b>Location</b>
<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/MS11-079.msp">http://www.microsoft.com/technet/security/Bulletin/MS11-079.msp</a>

**Relevant IPS 5500 Rules:** tln-102030.