



Securing Tomorrow's
Networks Today

TopResponse Threat Advisory

Release Date: November 09, 2010.

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection for the Microsoft Forefront Unified Access Gateway XSS Vulnerability (MS10-089,CVE-2010-3936).

Top Layer Products: IPS 5500 v4.X and higher.

Vulnerable Infrastructure: Forefront Unified Access Gateway 2010.

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 Forefront Unified Access Gateway (UAG) provides secure access to messaging, collaboration and other applications. A cross-site scripting (XSS) vulnerability exists that could allow specially crafted script code to run under the guise of the server. This is a non-persistent cross-site scripting vulnerability that could allow an attacker to issue commands to the UAG server in the context of the targeted user.

Recommended Action: Top Layer 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 Forefront UAG infrastructure. The rule is currently enabled in the "Recommended Server Protection" IPS Rule Set.

References: Use the following sources for additional information:

Additional Information	Location
Top Layer Support	http://www.toplayer.com/support
Microsoft Security Bulletin	http://www.microsoft.com/technet/security/bulletin/ms10-089.msp

Relevant TLN Rules: tln-102078

Relevant TopResponse Protection Pack(s): N/A