

TopResponse Threat Advisory

Release Date: January 18, 2012.

Purpose: The Corero TopResponse team is issuing an advisory, which provides information needed to block attacks targeting the Microsoft Anti-XSS Library Bypass Vulnerability (MS12-007,CVE-2012-0007).

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

Vulnerable Infrastructure: Microsoft Anti-Cross Site Scripting Library v3.x, Microsoft Anti-Cross Site Scripting Library v4.0.

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: The Microsoft Anti-Cross-Site Scripting (Anti-XSS) Library is a library designed to help developers protect ASP.NET applications from Cross-site Scripting (XSS) attacks. There exists a vulnerability in the way the library evaluates certain characters after an XSS-escaped character is detected. The reported vulnerability could allow an attacker to execute an XSS attack resulting in an unauthorized information disclosure by enticing a user to open a specially crafted web site.

Recommended Action: Corero recommends the following actions:

Download and apply Protection Pack 2012-01-11-01 (or later) to put this new protection into place. This will put into place protection for the Microsoft Anti-XSS Library Bypass 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-106409 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft Web Servers that use Microsoft Anti-XSS library.

References: Use the following sources for additional information:

Additional Information	Location
Corero Support	https://support.corero.com/
Microsoft Advisory	http://technet.microsoft.com/en-us/security/bulletin/ms12-007

Relevant IPS 5500 Rules: tln-106409.

Relevant TopResponse Protection Pack(s): 2012-01-11-01.