Threat Update Service* Advisory
October 9, 2012

Purpose: The Corero Security Active Response Team informs customers that existing IPS 5500 security features provide proactive protection against potential attacks targeting the Microsoft SQL Reflected XSS Vulnerability.

Issue: Microsoft SQL Server Report Manager does not properly validate request parameters on the Report Manager SQL Server site which can lead to a cross-site scripting attack. The reported vulnerability could allow an attacker to inject a client-side script into the user's instance of Internet Explorer and get elevated privileges or gain access to sensitive information on an unprotected system.

Recommended Action: Ensure that the associated rule is used to inspect traffic to the affected product infrastructure (as per the table below).

Issue Identifier	CVE-2012-2552, MS12-070
Vendor Advisory	http://technet.microsoft.com/security/bulletin/MS12-070
Identified In	October 2012 Microsoft Patch Tuesday release
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to get elevated privileges or gain access to sensitive information on an unprotected system.
Affected Products	SQL Server 2000 SQL Server 2005 SQL Server 2008 SQL Server 2008 R2 SQL Server 2012
Corero Products	IPS 5500 4.X and later.
Associated Rule	tln-102078
Associated Rule Set	This rule is automatically enabled in the “Strict Client Protection” and “Recommended Server Protection” rule sets.

* previously called TopResponse

https://support.corero.com Corero Network Security, Inc.
One Cabot Road, Hudson, MA 01749 +1-978-212-1500 • Fax +1-978-212-1600
• USA • Japan • Asia Pacific • EMEA