Threat Update Service* Advisory
July 10, 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 SharePoint scriptresx.ashx XSS Vulnerability.

Issue: Microsoft SharePoint does not properly handle malicious JavaScript elements within a specially crafted URL which can lead to a cross-site scripting attack. This could allow an attacker to get elevated privileges or gain access to sensitive information on an unprotected system.

Recommended Action: Apply the specified protection pack (or any later one) and ensure the associated rule is used to inspect traffic to the affected product infrastructure.

Issue Identifier	CVE-2012-1859, MS12-050
Vendor Advisory	http://technet.microsoft.com/security/bulletin/MS12-050
Identified In	July 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	Microsoft SharePoint Server 2010 (including Service Pack 1) SharePoint Foundation 2010 (including Service Pack 1) Microsoft Office Web Apps 2010 (including Service Pack 1)
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