# Threat Update Service* Advisory
## March 12, 2013

**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 XSS Vulnerability.

**Issue:** An elevation of privilege vulnerabiity exists in the Microsoft SharePoint Server as it does not properly handle malicious JavaScript elements within specially crafted site content. This could allow an attacker to execute arbitrary commands in the context of the administrative user on the site.

**Recommended Action:** Enable the specified rule and ensure that the rule is used to inspect traffic to the affected product infrastructure.

| | |
|---|---|
| **Issue Identifier** | CVE-2013-0083, MS13-024 |
| **Vendor Advisory** | http://technet.microsoft.com/security/bulletin/MS13-024 |
| **Risk Assessment** | Critical Vulnerability |
| **Threat Impact** | Remotely exploitable vulnerability that could allow an attacker to get elevated privileges or gain access to sensitive information. |
| **Affected Products** | Microsoft SharePoint Server 2010 Service Pack 1 |
| **Corero Products** | IPS 5500 and later. |
| **Associated Rule** | tln-102078 |
| **Associated Rule Set** | This rule is automatically enabled in the “Recommended Server Protection” and “Strict Client 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 