Threat Update Service* Advisory

May 13, 2014

Purpose: The Corero Security Active Response Team informs customers that the IPS 5500 has proactive coverage against attacks targeting the SharePoint 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 execute arbitrary code on an unprotected system in the security context of the W3WP service account.

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

Issue Identifier	CVE-2014-1754, MS14-022
Advisory	http://technet.microsoft.com/en-us/security/bulletin/ms14-022
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	Microsoft SharePoint Server 2013 Microsoft Office Web Apps 2013
Corero Products	IPS 5500 E-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.62 (build 007 and later), v6.80 (build 035 and later).
Associated Rule	tln-102078
Associated Rule Set	This rule is enabled in the “Recommended Server Protection” and “Strict Client Protection” rule sets.

* previously called TopResponse

