

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 Directory Traversal Vulnerability.

Issue: An elevation of privilege vulnerability exists in the Microsoft SharePoint Server as it does not properly validate user input. This could allow an attacker to gain access to sensitive information and execute arbitrary commands in the context of the currently logged in 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-2013-0084, 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 Microsoft SharePoint Foundation 2010 Service Pack 1
Corero Products	IPS 5500 and later.
Associated Rule	tln-102033
Associated Rule Set	This rule is automatically enabled in the "Strict Server Protection" rule set.

* previously called TopResponse