

Threat Update Service* Advisory

September 11, 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 System Center Configuration Manager Reflected XSS Vulnerability.

Issue: Microsoft System Center Configuration Manager does not properly handle malicious JavaScript elements within a specially crafted URL which can lead to a cross-site scripting attack. The reported vulnerability could allow an attacker to 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-2012-2536, MS12-062
Vendor Advisory	http://technet.microsoft.com/security/bulletin/MS12-062
Identified In	September 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 Systems Management Server 2003 Service Pack 3 Microsoft System Center Configuration Manager 2007 Service Pack 2
Corero Products	IPS 5500 4.X and later.
Associated Rule	tln-102030
Associated Rule Set	This rule is automatically enabled in the "Strict Server Protection" rule set.

* 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 Copyright 2012. All Rights Reserved.