Threat Update Service* Advisory

Protection Pack 2013-01-09-01 Released January 9, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Microsoft System Center Operations Manager Web Console XSS Vulnerability.

Issue: A non-persistent cross-site scripting (XSS) vulnerability exists in the Microsoft System Center Operations Manager because it does not properly validate input. This could allow an attacker to execute arbitrary script code in the context of the current user thereby gaining access to elevated privileges.

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-2013-0010, MS13-003
Vendor Advisory	http://technet.microsoft.com/en-us/security/bulletin/ms13-003
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 System Center Operations Manager 2007 Service Pack 1 Microsoft System Center Operations Manager 2007 R2
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106566
Associated Rule Set	This rule is automatically enabled in the “Recommended 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