Threat Update Service* Advisory

August 6, 2013

Purpose: The Corero Security Active Response Team informs customers that the IPS 5500 has proactive coverage against known attacks targeting the McAfee ePolicy Orchestrator Multiple Cross Site Scripting Vulnerabilities.

Issue: McAfee ePolicy Orchestrator contains multiple cross-site scripting (XSS) vulnerabilities that could allow an attacker to inject an arbitrary web script or HTML script that can be executed on the victim's machine. An attacker who successfully exploited these vulnerabilities could take complete control of an affected system.

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

Issue Identifier	CVE-2013-4883
Advisory	https://kc.mcafee.com/corporate/index?page=content&id=KB78824
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	McAfee ePolicy Orchestrator 4.6.6 and earlier ePO Extension for the McAfee Agent (MA) 4.5 through 4.6
Corero Products	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 013 and later), v6.80 (build 035 and later).
Associated Rule	tln-102078
Associated Rule Set	This rule is automatically enabled in the "Strict Client Protection" and "Recommended Server 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