

Threat Update Service* Advisory
Protection Pack 2013-10-06-01 Released October 6, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the AWS XMS 'what' Parameter Directory Traversal Vulnerability.

Issue: A path traversal vulnerability exists in the AWS XMS as it does not properly sanitize input passed to the 'what' parameter. This could allow an attacker to gain access to sensitive information by reading arbitrary files.

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-2013-2474
Advisory	http://www.securityfocus.com/bid/58753
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain access to sensitive information.
Affected Products	AWS XMS 2.5
Corero Products	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
Associated Rule	tln-106714
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 Copyright 2013. All Rights Reserved.