

Threat Update Service* Advisory
Protection Pack 2014-06-27-02 Released June 27, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the SAP Supplier Relationship Management umTestSSO.jsp Open Redirection Vulnerability.

Issue: A URL redirection vulnerability exists in la/umTestSSO.jsp in SAP Supplier Relationship Management. This could allow an attacker to carry out phishing attacks via a crafted url parameter.

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-2014-4159
Advisory	http://scn.sap.com/docs/DOC-8218
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to carry out phishing attacks.
Affected Products	SAP Supplier Relationship Management
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later), v6.82 (build 003 and later).
Associated Rule	tlIn-022197
Associated Rule Set	This rule is automatically enabled in the "Recommended Server Protection" rule set.

* previously called TopResponse

<http://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 2014. All Rights Reserved.