Threat Update Service* Advisory

Protection Pack 2013-05-28-01 Released May 28, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the SAP ConfigServlet Remote Code Execution Vulnerability.

Issue: An authentication bypass vulnerability exists in the SAP ConfigServlet in SAP NetWeaver. This could allow an attacker to execute arbitrary code on the system via a specially crafted GET request.

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	OSVDB: 92704
Advisory	http://www.osvdb.org/92704
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	SAP NetWeaver v7.00 and SAP NetWeaver v7.01
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025176
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