Threat Update Service* Advisory

Protection Pack 2013-03-01-03 Released March 1, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the SAP Netweaver Message Server WRITE_C Memory Corruption Vulnerability.

Issue: A remote code execution vulnerability exists in the SAP Netweaver msg_server.exe module as it does not properly process packets sent to the WRITE_C function. This could allow an attacker to cause a denial of service of an affected system.

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-2013-1593
Advisory	http://www.coresecurity.com/content/SAP-netweaver-msg-srv-multiple-vulnerabilities
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to cause a denial of service of an unprotected system.
Affected Products	SAP Netweaver 2004s SAP Netweaver 7.01 SR1 SAP Netweaver 7.02 SP06 SAP Netweaver 7.30 SP04
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106596
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