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 MsJ2EE_AddStatistics 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 _MsJ2EE_AddStatistics function. This could allow an attacker to execute arbitrary code on the victim's machine. An attacker who successfully exploited this vulnerability could take complete control 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-2013-1592
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 gain full control 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-106595
Associated Rule Set	This rule is automatically enabled in the "Recommended Server Protection" rule set.

* previously called TopResponse

