Threat Update Service* Advisory

Protection Pack 2012-09-25-02 Released September 25, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the SAP NetWeaver Dispatcher DiagTraceR3Info Buffer Overflow Vulnerability.

Issue: A remote code execution vulnerability exists in the Dialog processor in the Dispatcher in SAP NetWeaver. This could allow an attacker to execute arbitrary code on the remote machine by sending a specially crafted SAP Diag packet. 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-2012-2611
Vendor Advisory	http://scn.sap.com/docs/DOC-8218
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 7.0 EHP1 SAP NetWeaver 7.0 EHP2
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106509
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