Threat Update Service* Advisory

Protection Pack 2012-10-11-02 Released October 12, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the SAP NetWeaver HostControl Command Injection Vulnerability.

Issue: The SAPHostControl service fails to properly sanitize input passed to its SOAP management interface. This could allow an attacker to execute arbitrary code on the remote machine by injecting specially crafted commands. 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	SA50309
Advisory	http://secunia.com/advisories/50309/
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.x
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025141
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