Threat Update Service* Advisory

Protection Pack 2013-06-11-01 Released June 11, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the SAS Integration Technologies Client SASspk.dll Stack Based Overflow Vulnerability.

Issue: A stack buffer overflow vulnerability exists in the SAS Integration Technologies Client. This could allow an attacker to execute arbitrary code on the victim's machine and possibly 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	SAS: 49961
Advisory	http://support.sas.com/kb/49/961.html
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	SAS Integration Technologies Client
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106632
Associated Rule Set	This rule is automatically enabled in the "Strict Client Protection" rule set.

* previously called TopResponse

