Threat Update Service* Advisory

Protection Pack 2013-02-08-02 Released February 8, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Samsung Kies Remote Buffer Overflow Vulnerability.

Issue: A buffer overflow vulnerability exists in Samsung Kies because it does not properly validate user supplied input before copying it into a fixed length buffer. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted website. 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-2012-6429
Advisory	http://www.securityfocus.com/bid/57249/
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Samsung Kies 2.5.0.12114_1
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106578
Associated Rule Set	This rule is automatically enabled in the "Recommended Client 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