Threat Update Service* Advisory

Protection Pack 2013-12-09-02 Released December 10, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Apache Roller OGNL Injection Vulnerability.

Issue: A remote code execution vulnerability exists in Apache Roller as it does not properly sanitize the parameters to certain getText methods in the ActionSupport controller. This could allow an attacker to execute arbitrary OGNL expressions on the victim's machine.

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-2013-4212
Advisory	http://rollerweblogger.org/project/entry/apache_roller_5_0_2
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Apache Roller before 5.0.2
Corero Products	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
Associated Rule	tln-025219
Associated Rule Set	This rule is automatically enabled in the "Recommended Server Protection" rule set.

* previously called TopResponse

