Threat Update Service* Advisory

Protection Pack 2014-04-04-01 Released April 4, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Katello (Red Hat Satellite) users/update_roles Missing Authorization Vulnerability.

Issue: An elevation of privilege vulnerability exists in the Katello and Red Hat Satellite products. This could allow an attacker to gain the privileges of the administrator via the 'update_roles' action of the 'users' controller.

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-2013-2143
Advisory	http://cve.mitre.org/cgi-bin/cvename.cgi?name=2013-2143
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain elevated privileges on an unprotected system.
Affected Products	Katello and Red Hat Satellite
Corero Products	IPS 5500 E-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.62 (build 007 and later), v6.80 (build 035 and later).
Associated Rule	tln-025249
Associated Rule Set	This rule is automatically enabled in the “Strict 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