Threat Update Service* Advisory
Protection Pack 2012-07-27-01 Released July 27, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Oracle Java Applet2ClassLoader Class Unsigned Applet Code Execution Vulnerability.

Issue: The Deployment component in Java Runtime Environment (JRE) could allow an attacker to execute arbitrary code on the remote machine because it does not properly validate Java Web Start applications and Java applets. 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-2010-4452
Vendor Advisory	http://www.oracle.com/technetwork/topics/security/javacpufeb2011-304611.html
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Java Runtime Environment (JRE) in Oracle Java SE and Java for Business 6 Update 23 and prior versions
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025136
Associated Rule Set	This rule is automatically enabled in the “Recommended Client Protection” rule set.

* previously called TopResponse

