Threat Update Service* Advisory

Protection Pack 2013-05-03-01 Released May 3, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Oracle Java Runtime Environment Security Bypass Vulnerability.

Issue: A remote code execution vulnerability exists in the Oracle Java Runtime Environment. This could allow a remote attacker to execute arbitrary code on the system and possibly take complete control of the affected system via a crafted JAR file.

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-2013-2423
Advisory	http://www.oracle.com/technetwork/topics/security/javacpuapr2013-1928497.html
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on the system.
Affected Products	Oracle Java SE 7 Update 17 and earlier OpenJDK 7
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-022167
Associated Rule Set	This rule is automatically enabled in the “Recommended Client Protection” rule set.

* previously called TopResponse

