Threat Update Service* Advisory

Protection Pack 2012-08-31-02 Released August 31, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Oracle Java v7 Applet Remote Code Execution Vulnerability.

Issue: Java Runtime Environment (JRE) does not properly enforce SecurityManager restrictions. This could allow an attacker to execute arbitrary code on the remote machine by enticing the user to load a specially crafted applet file. 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-2012-4681
Vendor Advisory	http://www.oracle.com/technetwork/topics/security/alert-cve-2012-4681-1835715.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) component in Oracle Java SE 7 Update 6 and earlier Java Runtime Environment (JRE) component in Oracle Java SE 6 Update 34 and earlier
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025139
Associated Rule Set	This rule is automatically enabled in the “Recommended Client Protection” rule set.

* previously called TopResponse