Threat Update Service* Advisory

Protection Pack 2012-07-20-02 Released July 24, 2012

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

Issue: A type check vulnerability in the HotSpot bytecode verifier of the Java Runtime Environment (JRE) could allow an attacker to execute arbitrary code on the remote machine by sending a specially crafted JAR file and enticing the victim to open the 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-2012-1723
Vendor Advisory	http://www.oracle.com/technetwork/topics/security/javacpujun2012-1515912.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 7 update 4 and earlier Java Runtime Environment (JRE) in Oracle Java SE 6 update 32 and earlier Java Runtime Environment (JRE) in Oracle Java SE 5 update 35 and earlier Java Runtime Environment (JRE) 1.4.2_37 and earlier
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025135
Associated Rule Set	This rule is automatically enabled in the “Recommended Client Protection” rule set.

* previously called TopResponse

