Threat Update Service* Advisory

Protection Pack 2013-04-26-02 Released April 26, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Java Web Start Launcher ActiveX Control Memory Corruption Vulnerability.

Issue: A remote code execution vulnerability exists in the Java Runtime Environment (JRE) component in Oracle Java SE. This could allow an attacker to execute arbitrary code on the victim's machine and possibly 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-2013-2419
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 gain full control of an unprotected system.
Affected Products	Oracle Java SE 7 Update 17 and earlier Oracle Java SE 6 Update 43 and earlier Oracle Java SE 5.0 Update 41 and earlier
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106613
Associated Rule Set	This rule is automatically enabled in the "Recommended Client 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