Threat Update Service* Advisory

Protection Pack 2013-04-05-02 Released April 5, 2013

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

Issue: A remote code execution vulnerability exists in the color management (CMM) functionality in the 2D component in Oracle Java. This could allow a remote attacker to execute arbitrary code on the system and possibly take complete control of the affected system via an image with crafted raster parameters.

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-2013-1493
Advisory	http://www.oracle.com/ocom/groups/public/@otn/documents/webcontent/1915099.xml
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 15 and earlier Oracle Java SE 6 Update 41 and earlier Oracle Java SE 5.0 Update 40
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025165
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