

Threat Update Service* Advisory

Protection Pack 2013-12-19-02 Released December 20, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Oracle Java Incorrect ShortBandedRaster Size Checks Vulnerability.

Issue: A remote code execution vulnerability exists in Oracle Java. This could allow an attacker to execute arbitrary code on the victim's machine via a specially crafted JAR 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-2013-2472
Advisory	http://www.oracle.com/technetwork/topics/security/javacpujun2013-1899847.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 21 and earlier Oracle Java SE 6 Update 45 and earlier Oracle Java SE 5.0 Update 45 and earlier OpenJDK 7
Corero Products	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
Associated Rule	tIn-022189
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 Copyright 2013. All Rights Reserved.