

## Threat Update Service\* Advisory

### Protection Pack 2013-10-21-01 Released October 21, 2013

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Oracle Java IntegerInterleavedRaster Signed Integer Overflow Vulnerability.

**Issue:** An integer overflow vulnerability exists in the Java Runtime Environment (JRE) component in Oracle Java. This could allow an attacker to execute arbitrary code on an affected system. 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.

<b>Issue Identifier</b>	CVE-2013-2471
<b>Advisory</b>	<a href="http://www.oracle.com/technetwork/topics/security/javacpujun2013-1899847.html">http://www.oracle.com/technetwork/topics/security/javacpujun2013-1899847.html</a>
<b>Risk Assessment</b>	Critical Vulnerability
<b>Threat Impact</b>	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
<b>Affected Products</b>	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
<b>Corero Products</b>	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).
<b>Associated Rule</b>	tIn-022183
<b>Associated Rule Set</b>	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.