# Threat Update Service* Advisory

## Protection Pack 2012-12-21-02 Released December 21, 2012

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

**Issue:** A remote code execution vulnerability exists in the JAX-WS classes in the JRE component of Oracle Java. This could allow a remote attacker to execute arbitrary code outside of the Java sandbox 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-2012-5076 |
| **Advisory** | http://www.oracle.com/technetwork/topics/security/javacpuoct2012-1515924.html |
| **Risk Assessment** | Critical Vulnerability |
| **Threat Impact** | Remotely exploitable vulnerability that could allow an attacker to gain control of an unprotected system. |
| **Affected Products** | Java Runtime Environment (JRE) in Oracle Java SE 7 Update 7 and earlier |
| **Corero Products** | IPS 5500 E-Series and later. |
| **Associated Rule** | tln-106563 |
| **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 