

Threat Update Service* Advisory
Protection Pack 2013-09-11-01 Released September 11, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Oracle Java lookupByteBI Function Heap Buffer Overflow Vulnerability.

Issue: A heap buffer overflow vulnerability exists in the Java Runtime Environment (JRE) component in Oracle Java SE. This could allow an attacker to execute arbitrary code on the system and possibly take complete control of the system via a specially crafted CLASS file.

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-2013-2470
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 execute arbitrary code on the 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-106687
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.