Threat Update Service* Advisory

Protection Pack 2013-07-19-01 Released July 19, 2013

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

Issue: A remote code injection vulnerability exists in Oracle Sun Java Web Start. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted JNLP 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-2012-1533
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 full control of an unprotected system.
Affected Products	Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier, and 6 Update 35 and earlier
Corero Products	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 013 and later), v6.80 (build 035 and later).
Associated Rule	tln-025185
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