Threat Update Service* Advisory

Protection Pack 2014-02-07-03 Released February 7, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Oracle Fusion Middleware Reports Developer Remote Security Vulnerability.

Issue: An information disclosure and file upload vulnerability exists in the Oracle Reports Developer component in Oracle Fusion Middleware. This could allow an attacker to execute arbitrary scripts on the affected system via a specially crafted JSP 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-2012-3152, CVE-2012-3153
Advisory	http://www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	Oracle Reports Developer component in Oracle Fusion Middleware 11.1.1.4, 11.1.1.6, and 11.1.2.0
Corero Products	IPS 5500 E-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.62 (build 007 and later), v6.80 (build 035 and later).
Associated Rule	tln-106784
Associated Rule Set	This rule is automatically enabled in the “Recommended Server 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