Threat Update Service* Advisory

Protection Pack 2013-09-05-01 Released September 6, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Oracle CVE-2013-3763 Endeca Server Remote Command Execution Vulnerability.

Issue: A remote code execution vulnerability exists in the Oracle Endeca Server component in Oracle Fusion Middleware. This could allow an attacker to execute arbitrary code on the system and possibly take complete control of the system via the createDataStore method from the controlSoapBinding web service.

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-2013-3763
Advisory	http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.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 Fusion Middleware 7.4.0 and 7.5.1.1
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	tln-025199
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