

Threat Update Service* Advisory

Protection Pack 2014-07-24-01 Released July 25, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Oracle Event Processing FileUploadServlet Arbitrary File Upload Vulnerability.

Issue: A file upload vulnerability exists in the Oracle Event Processing component in Oracle Fusion Middleware. This could allow an attacker to upload and execute arbitrary files on the victim's machine via a specially crafted request.

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-2014-2424
Advisory	http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to upload arbitrary files to an unprotected system.
Affected Products	Oracle Event Processing component in Oracle Fusion Middleware 11.1.1.7.0
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later), v6.82 (build 003 and later).
Associated Rule	tIn-025270
Associated Rule Set	This rule is automatically enabled in the "Recommended Server Protection" rule set.

* previously called TopResponse

<http://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 2014. All Rights Reserved.