

CVE-2012-3152

Oracle Fusion Middleware Unspecified Vulnerability

Exigent

CISA KEV since Nov 3, 2021

Actively exploited

Public exploit module (Metasploit)

Unspecified vulnerability in the Oracle Reports Developer component in Oracle Fusion Middleware 11.1.1.4, 11.1.1.6, and 11.1.2.0 allows remote attackers to affect confidentiality and integrity via unknown vectors related to Report Server Component. NOTE: the previous information is from the October 2012 CPU. Oracle has not commented on claims from the original researcher that the URLPARAMETER functionality allows remote attackers to read and upload arbitrary files to reports/rwsservlet, and that this issue occurs in

EVRS

86/100

Immediate priority

CVSS V3.1

9.1

Critical · NVD

EPSS

0.988

99.93rd percentile · FIRST

CISA DEADLINE

May 3, 2022

KEV since 2021 · listed over a year

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.988 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent No patch reported by the connected remediation source**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

earlier versions. NOTE: this can be leveraged with CVE-2012-3153 to execute arbitrary code by uploading a .jsp file.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
fusion middleware	11.1.1.4.0 11.1.1.6.0 11.1.2.0	no fixed version listed	NVD

Sources

NVD nvd.nist.gov/vuln/detail/CVE-2012-3152ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2012-3130CISA KEV cisa.gov/known-exploited-vulnerabilities-catalogCurrent data evulnable.com/vulnerability-management/cve/CVE-2012-3152

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.