

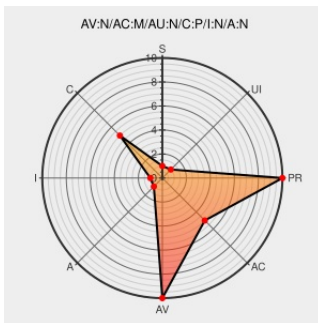


CVE-2015-4845

Published on: 10/21/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:06 PM UTC

CVE-2015-4845

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [E-business Suite](#) from [Oracle](#) contain the following vulnerability:

Unspecified vulnerability in the Oracle Application Object Library component in Oracle E-Business Suite 11.5.10.2, 12.0.6, 12.1.3, 12.2.3, and 12.2.4 allows remote attackers to affect confidentiality via vectors related to Java APIs - AOL/J. NOTE: the previous information is from the October 2015 CPU. Oracle has not commented on third-

party claims that this issue allows remote attackers to enumerate database users via a series of requests to Aoljtest.js.

CVE-2015-4845 has been assigned by [secalert_us@oracle.com](#) to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

NONE

NONE

CVE References

Description

Tags

Link

Oracle Critical Patch Update - October 2015

[Patch](#)
[Vendor Advisory](#)
[www.oracle.com](#)
[text/html](#)

[CONFIRM](#)
[www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html](#)

Oracle E-Business Suite CVE-2015-4845 User Enumeration Vulnerability

[cve.report \(archive\)](#)
[text/html](#)

[BID 77249](#)

[ERPSCAN-15-025] Oracle E-Business Suite - Database user enumeration vulnerability

[erpscan.io](#)
[text/html](#)

[MISC erpscan.io/advisories/erpscan-15-025-oracle-e-business-suite-database-user-enumeration-vulnerability/](#)

Oracle E-Business Suite Bugs Let Remote Users

[www.securitytracker.com](#)

[SECTRAK 1033877](#)

text/html

seclists.org

text/html



packetstormsecurity.com

text/html

PS

www.securityfocus.com

text/html

comment@cve.report

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	E-business Suite	11.5.10.2	All	All	All
Application	Oracle	E-business Suite	12.0.6	All	All	All
Application	Oracle	E-business Suite	12.1.3	All	All	All
Application	Oracle	E-business Suite	12.2.3	All	All	All
Application	Oracle	E-business Suite	12.2.4	All	All	All
Application	Oracle	E-business Suite	11.5.10.2	All	All	All
Application	Oracle	E-business Suite	12.0.6	All	All	All
Application	Oracle	E-business Suite	12.1.3	All	All	All
Application	Oracle	E-business Suite	12.2.3	All	All	All
Application	Oracle	E-business Suite	12.2.4	All	All	All

```
cpe:2.3:a:oracle:e-business_suite:11.5.10.2:::*:*:*:*:*
```

```
cpe:2.3:a:oracle:e-business_suite:12.0.6:::*:*:*:*:*
```

cpe:2.3:a:oracle:e-business_suite:12.1.3:*:*:*:*:*:*

cpe:2.3:a:oracle:e-business_suite:12.2.3:*:*:*:*:*:*

cpe:2.3:a:oracle:e-business_suite:12.2.4:*:*:*:*:*:*

```
cpe:2.3:a:oracle:e-business suite:11.5.10.2:::*:*:*:*:*:
```

```
cpe:2.3:a:oracle:e-business suite:12.0.6:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:e-business suite:12.1.3:*:*:*:*:*:
```

```
any22:procedures business suite:12 2 2.**.*.*.*.*.*.
```

cpe:2.3:a:oracle:e-business_suite:12.2.3:1:1:1:1:1:1:1

cpe:2.3:a:oracle:e-business_suite:12.2.4:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)