

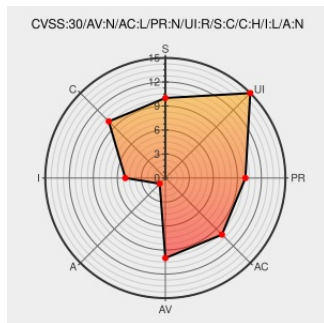


# CVE-2020-2890

Published on: 04/15/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:09 PM UTC

## CVE-2020-2890

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

Certain versions of [Applications Framework](#) from [Oracle](#) contain the following vulnerability:

Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: Diagnostics). Supported versions that are affected are 12.1.3 and 12.2.3-12.2.9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Framework. Successful

attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Applications Framework accessible data as well as unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).

CVE-2020-2890 has been assigned by secalert\_us@oracle.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Oracle Corporation - Applications Framework** version = **12.1.3**

Affected Vendor/Software: **Oracle Corporation - Applications Framework** version = **12.2.3-12.2.9**

CVSS3 Score: **8.2 - HIGH**

| Attack Vector  | Attack Complexity      | Privileges Required | User Interaction    |
|----------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b> | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope          | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>CHANGED</b> | <b>HIGH</b>            | <b>LOW</b>          | <b>NONE</b>         |

CVSS2 Score: **5.8 - MEDIUM**

| Access Vector | Access Complexity | Authentication |
|---------------|-------------------|----------------|
|---------------|-------------------|----------------|

NETWORK

MEDIUM

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

PARTIAL

PARTIAL

NONE

CVE References

Description

Tags

Link

Oracle Critical Patch Update Advisory - April 2020

Vendor Advisory

www.oracle.com

text/html

MISC

www.oracle.com/security-alerts/cpuapr2020.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto: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

Applications Framework

12.1.3

All

All

All

Application

Oracle

Applications Framework

12.1.3

All

All

All

Application

Oracle

Applications Framework

All

All

All

All

cpe:2.3:a:oracle:applications\_framework:12.1.3:\*:\*:\*:\*:\*:

cpe:2.3:a:oracle:applications\_framework:12.1.3:\*:\*:\*:\*:\*:

cpe:2.3:a:oracle:applications\_framework:\*:\*:\*:\*:\*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →