



CVE-2020-14611

Published on: 07/15/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:01 PM UTC

CVE-2020-14611

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L



Certain versions of [Webcenter Portal](#) from [Oracle](#) contain the following vulnerability:

Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Composer). Supported versions that are affected are 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks of this

vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Portal accessible data as well as unauthorized read access to a subset of Oracle WebCenter Portal accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebCenter Portal. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L).

CVE-2020-14611 has been assigned by [secalert_us@oracle.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Oracle Corporation](#) - **WebCenter Portal** version = **12.2.1.3.0**

Affected Vendor/Software: [Oracle Corporation](#) - **WebCenter Portal** version = **12.2.1.4.0**

CVSS3 Score: **8.6 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	LOW	HIGH	LOW

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE

Confidentiality Impact

Integrity Impact

Availability Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Oracle Critical Patch Update Advisory - July 2020

Tags

Patch

Vendor Advisory

www.oracle.com

text/html

Link

MISC www.oracle.com/security-alerts/cpujul2020.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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type

Vendor

Product

Version

Update

Edition

Language

Application

Oracle

Webcenter Portal

12.2.1.3.0

All

All

All

Application

Oracle

Webcenter Portal

12.2.1.4.0

All

All

All

Application

Oracle

Webcenter Portal

12.2.1.3.0

All

All

All

Application

Oracle

Webcenter Portal

12.2.1.4.0

All

All

All

cpe:2.3:a:oracle:webcenter_portal:12.2.1.3.0:*:*:*:*:*:

cpe:2.3:a:oracle:webcenter_portal:12.2.1.4.0:*:*:*:*:*:

cpe:2.3:a:oracle:webcenter_portal:12.2.1.3.0:*:*:*:*:*:

cpe:2.3:a:oracle:webcenter_portal:12.2.1.4.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →