



CVE-2019-3012

Published on: 10/16/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:42 PM UTC

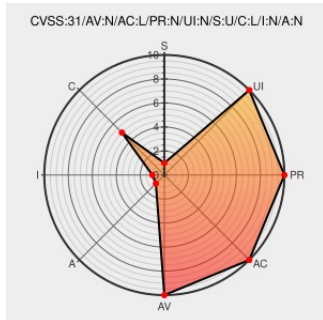
CVE-2019-3012

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Business Intelligence](#) from [Oracle](#) contain the following vulnerability:

Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Fusion Middleware (component: BI Platform Security). Supported versions that are affected are 11.1.1.9.0, 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 Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).

CVE-2019-3012 has been assigned by [secalert_us@oracle.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Oracle Corporation - Business Intelligence Enterprise Edition version = 11.1.1.9.0**

Affected Vendor/Software: **Oracle Corporation - Business Intelligence Enterprise Edition version = 12.2.1.3.0**

Affected Vendor/Software: **Oracle Corporation - Business Intelligence Enterprise Edition version = 12.2.1.4.0**

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE

Confidentiality Impact

Integrity Impact

Availability Impact

PARTIAL

NONE

NONE

CVE References

Description

Tags

Link

Oracle Critical Patch Update Advisory - October 2019

Patch

www.oracle.com

text/html

MISC

www.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.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	Business Intelligence	11.1.1.9.0	All	All	All
Application	Oracle	Business Intelligence	12.2.1.3.0	All	All	All
Application	Oracle	Business Intelligence	12.2.1.4.0	All	All	All
Application	Oracle	Business Intelligence	11.1.1.9.0	All	All	All
Application	Oracle	Business Intelligence	12.2.1.3.0	All	All	All
Application	Oracle	Business Intelligence	12.2.1.4.0	All	All	All

cpe:2.3:a:oracle:business_intelligence:11.1.1.9.0:*:*:*:enterprise:*:*:*:

cpe:2.3:a:oracle:business_intelligence:12.2.1.3.0:*:*:*:enterprise:*:*:*:

cpe:2.3:a:oracle:business_intelligence:12.2.1.4.0:*:*:*:enterprise:*:*:*:

cpe:2.3:a:oracle:business_intelligence:11.1.1.9.0:*:*:*:enterprise:*:*:*:

cpe:2.3:a:oracle:business_intelligence:12.2.1.3.0:*:*:*:enterprise:*:*:*:

cpe:2.3:a:oracle:business_intelligence:12.2.1.4.0:*:*:*:enterprise:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

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](#)