CVE Details

The ultimate security vulnerability datasource

Vulnerability Feeds & WidgetsNew

www.itsecdb.com

The approved seeming value willing accessor

<u>Home</u>

Browse :

Vendors

<u>Products</u>
<u>Vulnerabilities By Date</u>
<u>Vulnerabilities By Type</u>

Reports:

CVSS Score Report
CVSS Score Distribution

Search:

Vendor Search

Product Search
Version Search

Vulnerability Search

By Microsoft References

Top 50:

Vendors

Vendor Cvss Scores

Products

Product Cvss Scores
Versions

Other:

Microsoft Bulletins

Bugtraq Entries
CWE Definitions

About & Contact

Feedback

CVE Help

FAO

<u>Articles</u>

External Links:

NVD Website
CWE Web Site

View CVE:

Go

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID:

(e.g.: 12345)

Search By Microsoft Reference ID:

Go

(e.g.: ms10-001 or 979352)

Oracle » Database » 12.2.0.1 : Security Vulnerabilities

Cpe Name:cpe:/a:oracle:database:12.2.0.1

Copy Results Download Results

#	CVE ID	CWE	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-2619	284			2019-	2019-	4.6	None	Local	Low	Not required	Partial	Partial	Partial
					04-23	04-25								

Vulnerability in the Portable Clusterware component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows high privileged attacker having Grid Infrastructure User privilege with logon to the infrastructure where Portable Clusterware executes to compromise Portable Clusterware. While the vulnerability is in Portable Clusterware, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Portable Clusterware. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).

2 <u>CVE-2019-2444</u> <u>284</u> 2019- 2019- 4.4 None Local Medium Not required Partial Partial Partial 01-16 01-18

Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.2.0.1 and 18c. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where Core RDBMS executes to compromise Core RDBMS. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Core RDBMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Core RDBMS. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H).

3 <u>CVE-2019-2406</u> <u>284</u> 2019- 2019- 6.5 None Remote Low Single system Partial Partial Partial 01-16 01-18

Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows high privileged attacker having Create Session, Execute Catalog Role privilege with network access via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in takeover of Core RDBMS. CVSS 3.0 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).

4 <u>CVE-2017-10321</u> <u>284</u> 2017- 2017- 4.6 None Local Low Not required Partial Partial Partial 10-19 10-24

Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Easily exploitable vulnerability allows low privileged attacker having Create session privilege with logon to the infrastructure where Core RDBMS executes to compromise Core RDBMS. While the vulnerability is in Core RDBMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Core RDBMS. Note: This score is for Windows platform version 11.2.0.4 of Database. For Windows platform version 12.1.0.2 and Linux, the score is 7.8 with scope Unchanged. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).

5 <u>CVE-2017-10292</u> <u>264</u> 2017- 2017- 10-19 10-24 Low Single system None Partial None

Vulnerability in the RDBMS Security component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Easily exploitable vulnerability allows high privileged attacker having Create User privilege with logon to the infrastructure where RDBMS Security executes to compromise RDBMS Security. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of RDBMS Security accessible data. CVSS 3.0 Base Score 2.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).

Vulnerability in the OJVM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Easily exploitable vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise OJVM. While the vulnerability is in OJVM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of OJVM. Note: This score is for Windows platforms. On non-Windows platforms Scope is Unchanged, giving a CVSS Base Score of 8.8. CVSS 3.0 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).

7 <u>CVE-2017-10190</u> <u>284</u> 2017- 2017- 4.3 None Local Low Single system Partial Partial Partial 10-19 10-23

Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Easily exploitable vulnerability allows high privileged attacker having Create Session, Create Procedure privilege with logon to the infrastructure where Java VM executes to compromise Java VM. While the vulnerability is in Java VM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java VM. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).

Total number of vulnerabilities : **7** Page : **1** (This Page)

CVE is a registred trademark of the MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. CWE is a registred trademark of the MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site.

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.