Oracle » Database » 12.2.0.1 : Security Vulnerabilities

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

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

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

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	CVE-2019-2444	284			2019-01-16	2019-01-18	4.4	None	Local	Medium	Not required	Partial	Partial	Partial

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	CVE-2019-2406	284			2019-01-16	2019-01-18	6.5	None	Remote	Low	Single system	Partial	Partial	Partial

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	CVE-2017-10321	284			2017-10-19	2017-10-24	4.6	None	Local	Low	Not required	Partial	Partial	Partial

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	CVE-2017-10292	264			2017-10-19	2017-10-24	1.7	None	Local	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).

6	CVE-2017-10202	284			2017-08-08	2017-08-18	6.5	None	Remote	Low	Single system	Partial	Partial	Partial

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	CVE-2017-10190	284			2017-10-19	2017-10-23	4.3	None	Local	Low	Single system	Partial	Partial	Partial

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)