



CVE-2017-10292

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary	
CVE	CVE-2017-10292
State	PUBLISHED
Assigner	oracle
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-19 17:29:02 UTC
Updated	2025-04-20 01:37:25 UTC
Description	Vulnerability in the RDBMS Security component of Oracle Database Server. Supported versions that are affected are 11.2.0.4.0 and 11.2.0.3.0. The vulnerability allows a user with the CREATE USER privilege to execute a malicious SQL statement that can cause a denial of service (DoS) condition. The vulnerability is due to a buffer overflow in the RDBMS Security component. An attacker can exploit this vulnerability by sending a malicious SQL statement to the database. The attacker can cause a denial of service (DoS) condition by causing the database to crash. The vulnerability is present in the RDBMS Security component of Oracle Database Server. Supported versions that are affected are 11.2.0.4.0 and 11.2.0.3.0. The vulnerability is due to a buffer overflow in the RDBMS Security component. An attacker can exploit this vulnerability by sending a malicious SQL statement to the database. The attacker can cause a denial of service (DoS) condition by causing the database to crash.

Risk And Classification

Primary CVSS: v3.0 2.3 LOW from nvd@nist.gov

CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N

Problem Types: CWE-269 | 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.

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	2.3	LOW	CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N
2.0	nvd@nist.gov	Primary	1.7		AV:L/AC:L/Au:S/C:N/I:P/A:N

CVSS v3.0 Breakdown	
Attack Vector	Local
Attack Complexity	Low
Privileges Required	High
User Interaction	None
Scope	Unchanged
Confidentiality	None

ntegrity

Low

Availability

None

CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

Single

Confidentiality

None

ntegrity

Partial

Availability

None

AV:L/AC:L/Au:S/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Database	11.2.0.4	All	All	All
Application	Oracle	Database	12.1.0.2	All	All	All
Application	Oracle	Database	12.2.0.1	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Oracle Corporation	Oracle Database	affected 11.2.0.4	Not specified
CNA	Oracle Corporation	Oracle Database	affected 12.1.0.2	Not specified
CNA	Oracle Corporation	Oracle Database	affected 12.2.0.1	Not specified

References	
Reference	Source
Oracle Database Server CVE-2017-10292 Local Security Vulnerability	af854a3a-2127-422b-91ae-
Oracle Critical Patch Update - October 2017	af854a3a-2127-422b-91ae-
Oracle Database Bugs Let Local Users Gain Elevated Privileges and Access and Modify Data - SecurityTracker	af854a3a-2127-422b-91ae-

CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
No vendor comments have been submitted for this CVE.	
There are currently no legacy QID mappings associated with this CVE.	

© [CVE.report](#) 2026 |

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.

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)