Agent 2 Oracle plugin TNS connection string injection via the 'service' parameter

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

Summary

CVE	CVE-2026-23927
State	PUBLISHED
Assigner	Zabbix
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-06 08:16:02 UTC
Updated	2026-05-06 08:16:02 UTC
Description	A user able to connect to Agent 2 can inject an Oracle TNS connection string via the 'service' parameter. This can lead to A

Risk And Classification

Primary CVSS: v4.0 5.1 MEDIUM from security@zabbix.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:N/VI:L/VA:N/SC:H/SI:H/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-522 | CWE-522 CWE-522: Insufficiently Protected Credentials

Version	Source	Type	Score	Severity	Vector
4.0	security@zabbix.com	Secondary	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:N/VI:L/VA:N/SC:H/SI:H/SA:N/E:X
4.0	CNA	CVSS	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:N/VI:L/VA:N/SC:H/SI:H/SA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

High

User Interaction

None

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:N/VI:L/VA:N/SC:H/SI:H/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Zabbix	Zabbix	affected 6.0.0 6.0.44 git	Not specified
CNA	Zabbix	Zabbix	affected 7.0.0 7.0.23 git	Not specified
CNA	Zabbix	Zabbix	affected 7.4.0 7.4.7 git	Not specified

References

Reference	Source	Link	Tags
support.zabbix.com/browse/ZBX-27759	security@zabbix.com	support.zabbix.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Zabbix wants to thank kelsier from clocktwice.com for submitting this report on the HackerOne bug bounty platform. (en)

Additional Advisory Data

Solutions

CNA: Update the affected components to their respective fixed versions.

Workarounds

CNA: Don't use named sessions for Oracle database monitoring.

There are currently no legacy QID mappings associated with this CVE.