



ZABBIX BUGS AND ISSUES / ZBX-27759

Agent 2 Oracle plugin TNS connection string injection via the 'service' parameter (CVE-2026-23927)

Details

Type:	Defect (Security)	Resolution:	Fixed
Priority:	Minor	Fix Version/s:	None
Affects Version/s:	None		
Component/s:	Agent2 plugin (G)		
Labels:	None		

Description

CVE ID	CVE-2026-23927
CVSS score	5.1 (Medium)
CVSS vector	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
Affected components	Agent2
Summary	Agent 2 Oracle plugin TNS connection string injection via the 'service' parameter
Description	A user able to connect to Agent 2 can inject an Oracle TNS connection string via the 'service' parameter. This can lead to Agent 2 connecting to an attacker-controlled server and leaking Oracle database credentials if they are saved in a named session.
Known attack vectors	An attacker sending malicious requests to Agent 2 monitoring an Oracle database.
Affected and fix version/s	Affected: 6.0.0 - 6.0.44 → Fixed: 6.0.45 Affected: 7.0.0 - 7.0.23 → Fixed: 7.0.24 Affected: 7.4.0 - 7.4.7 → Fixed: 7.4.8
Mitigation	Update the affected components to their respective fixed versions.
Workarounds	Don't use named sessions for Oracle database monitoring.
Acknowledgements	Zabbix wants to thank kelsier from clockwice.com for submitting this report on the HackerOne bug bounty platform.

Activity

-
-
-

People

- Assignee:
- Zabbix Support Team
- Reporter:
- Janis Nulle
- Votes:
- 0 Vote for this issue
- Watchers:
- 1 Start watching this issue

Dates

Created:
1 hour ago

5/6/26, 8:08 AM

[ZBX-27759] Agent 2 Oracle plugin TNS connection string injection via the 'service' parameter (CVE-2026-23927) - ...

Updated:

1 hour ago

Resolved:

1 hour ago