TECHNICAL BRIEF

Prepared Nov 27, 2026, 5:34 PM PST

Oracle: CVE-2026-114819 Oracle Text flaw in Oracle Database (Create Session to code execution chain)

Status: Recovering / monitoring

Started Nov 17, 2026, 1:31 PM PST · Oracle's estimate: Fix already released; no further fix date

WHERE THINGS STAND

Oracle has released the fix for CVE-2026-114819 in its November 17, 2026 update. Public research published around November 20 shows a chain with an October-patched Oracle REST Data Services flaw, with no attacks observed; BIS has had reports of the chain.

Affected: Oracle Database Server 19c (19.3-19.32), Oracle Database Server 21c (21.3-21.24), Oracle Database Server 23ai (23.4.0-23.26.3), Oracle Text, Oracle REST Data Services (GraphQL, CVE-2026-91609)

REFERENCE NUMBERS

ID	TYPE	SEVERITY	EXPLOITED	LINK
CVE-2026-114819	CVE	CVSS 9.9 · critical	No	https://www.oracle.com/security-alerts/cspunov2026.html
CVE-2026-114848	CVE	CVSS 9.9 · critical	No	https://www.oracle.com/security-alerts/cspunov2026.html
CVE-2026-91609	CVE	—	No	https://www.oracle.com/security-alerts/cpuoct2026.html
Oracle CSPU November 2026	vendor	—	No	https://www.oracle.com/security-alerts/cspunov2026.html

AFFECTED VERSIONS AND FIXES

Every publicly affected version line found. Rows marked (BIS) are systems BIS runs.

PRODUCT / DISTRIBUTION	AFFECTED	FIXED IN	STATUS	SOURCE
(BIS) Oracle Database Server 19c	19.3-19.32 (some trackers say 19.33)	Nov 2026 CSPU (released 17 Nov 2026)	**FIXED**	Oracle Critical Security Patch Update Advisory - November 2026, 2026-11-17
(BIS) Oracle Database Server 21c	21.3-21.24	Nov 2026 CSPU (released 17 Nov 2026)	**FIXED**	Oracle Critical Security Patch Update Advisory - November 2026, 2026-11-17
(BIS) Oracle Database Server 23ai	23.4.0-23.26.3	Nov 2026 CSPU (released 17 Nov 2026)	**FIXED**	Oracle Critical Security Patch Update Advisory - November 2026, 2026-11-17

WORKAROUNDS UNTIL A FIX IS INSTALLED

- Oracle lists no workaround for these flaws, per reporting on the advisory; apply the November 2026 patch.
- Keep Oracle REST Data Services off public networks until the October 2026 update is confirmed (general hardening).

Questions? Contact BIS Computer Solutions, Inc.

Phone: +1-818-248-5023 · Fax: +1-818-249-1169 · Email: support@biscomputer.com · Web: www.biscomputer.com

HOW TO CHECK IF A SYSTEM IS AFFECTED

```
SELECT banner FROM v$version; (then compare with the November 2026 patch level)
opatch lspatches (self-managed installs; look for the November 2026 patch)
OCI console: DB system patch history (managed DBaaS)
```

ROOT CAUSE

Flaw in the Oracle Text component: a user with Create Session over Oracle Net can take over Oracle Text. The researcher's chain adds a GraphQL flaw in Oracle REST Data Services that is reachable without login on an exposed endpoint.

EXPLOITATION

No exploitation confirmed; the research reports no attacks observed, and the CVE record says active exploitation has not been confirmed.

WHAT THE IT COMMUNITY IS SAYING

The only posts I could find on this flaw repeat the researcher's claim that Oracle patched CVE-2026-114819, which he reported, and The Hacker News promotes his research on a pre-auth chain against Oracle. No admin reported impact, asked for help, shared a workaround, or reported exploitation, and no candidate posts were supplied to check. The LinkedIn items are reactions on profile activity feeds, not posts with their own URLs, so I did not list them.

From public posts by IT administrators; not confirmed by the vendor.

TIMELINE (NEWEST FIRST)

Nov 27, 2026, 5:34 PM PST

Oracle's November 17, 2026 patch update fixes CVE-2026-114819, and research published around November 20 links it to a second, October-patched Oracle REST Data Services flaw; no attacks were observed.

Nov 27, 2026, 4:07 PM PST

One new item: a third-party KEV list (Saktec) claims CISA has listed CVE-2026-114819, which conflicts with SecurityOnline and is unconfirmed; the Oracle fix is unchanged.

Nov 27, 2026, 4:01 AM PST

One small new point: The Hacker News says Oracle rates the REST Data Services flaw, CVE-2026-91609, as not exploitable without a login on its own; the Oracle fix status is unchanged.

Nov 26, 2026, 3:55 PM PST

Oracle's own November advisory text now confirms that 23.26.4 is in scope for CVE-2026-114822 and gives a count of remotely exploitable patches; the chained exploit remains unconfirmed by Oracle and there is still no exploitation report.

Nov 26, 2026, 7:50 AM PST

One small new item: Oracle's security alerts index now lists the October 2026 CPU at Rev 4 (25 November); the Oracle fix status is unchanged.

Nov 26, 2026, 3:48 AM PST

One small new point: a CISA ADP record lists CVE-2026-91609 with exploitation "none"; Oracle's fix status is unchanged.

Nov 25, 2026, 7:44 PM PST

One small new point: The Hacker News says cutting back temporary-table privileges does not close the Oracle path, and Oracle's fix status is unchanged.

Nov 24, 2026, 11:34 PM PST

The Hacker News article now confirms the research was published November 18, and says the full attack chains were not independently reproduced; Oracle's fix status is unchanged.

Nov 24, 2026, 7:28 AM PST

One new detail: a Depthfirst write-up says the Oracle chain runs commands as the database's OS service user (researcher's claim, unconfirmed by Oracle); Oracle's fix status is unchanged.

Nov 24, 2026, 3:27 AM PST

New since the last check: Oracle's November advisory lists APEX and REST Data Services patch details, and a

third-party GitHub pull request names one more CVE (unconfirmed); the Oracle fix status is unchanged.

Nov 19, 2026, 4:00 PM PST

Researcher publishes chain with ORDS flaw; no attacks observed (The Hacker News)

Nov 17, 2026, 1:31 PM PST

CVE-2026-114819 published; fixed in November CSPU (Oracle)

Oct 19, 2026, 5:00 PM PDT

Oracle October update fixes CVE-2026-91609 (ORDS GraphQL) (Oracle)

SOURCES

Researcher Demonstrates Database RCE Exploits Affecting PostgreSQL, MySQL and Oracle — https://thehackernews.com/2026/11/researcher-demonstrates-database-rce.html