THREAT INTELLIGENCE BRIEFING

CVE-2026-114784

Übernahme von Oracle Business Intelligence ohne Anmeldung.

Eine Lücke in der Komponente Platform Security von Oracle Business Intelligence Enterprise Edition (OBIEE) lässt sich laut Oracle leicht ausnutzen: Ein Angreifer ohne Anmeldung kann das System über HTTP übernehmen, mit Folgen auch für angebundene Produkte. Oracle hat die Lücke am 17.11.2026 geschlossen und bewertet sie mit dem Höchstwert 10,0. Eine Ausnutzung ist bisher nicht bekannt.

> **Geschäftsrisiko:** Übernahme der Reporting-Plattform mit Zugriff auf Finanz-, Vertriebs- und Personaldaten sowie auf die Zugangsdaten zu den angebundenen Datenquellen; dazu ein ggf. meldepflichtiger Vorfall nach NIS-2 / DSGVO.

10,0 / 10

KRITISCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H` – aus dem Netz über HTTP, ohne Anmeldung und ohne Mitwirkung eines Nutzers, mit voller Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Der Angriff kann laut Oracle auch weitere Produkte erheblich treffen (Scope Changed). Basiswert laut Oracle als CNA, im NVD übernommen.

AUSNUTZUNG	BETROFFEN	HANDLUNGSBEDARF
Nicht bekannt (Stand 17.11.2026)	Oracle BI Enterprise Edition 8.2.0.0.0 und 26.01.0.0.0	Dringend – vor Ausnutzungsbeginn patchen

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

10,0 · KRITISCH
CVSS-Schweregrad · höchster Wert

Ohne Anmeldung
HTTP · Komponente Platform Security

Nicht bekannt
Ausnutzung · nicht in CISA KEV · kein PoC öffentlich

CSPU Nov. 2026
Patch seit 17.11.2026 · My Oracle Support CPU451

Die Ursache: Die betroffene Komponente ist laut Oracle **Platform Security** in Oracle Business Intelligence Enterprise Edition. Ein **nicht authentifizierter Angreifer** mit Netzwerkzugang über **HTTP** kann die Lücke leicht ausnutzen und das System **übernehmen**; der Angriff kann weitere Produkte erheblich treffen (Scope Changed). Oracle nennt keine weiteren technischen Details.

ANGRIFFSKETTE

01	02	03	04
OBIEE erreichbar – Analytics-Oberfläche per HTTP ansprechbar	**Präparierte Anfrage** – an Platform Security, ohne Anmeldung	**Übernahme** – Kontrolle über die BI-Plattform	**Datenzugriff** – Berichte, Datenquellen, hinterlegte Zugangsdaten

Betroffenheit & Fixversionen

Produkt · Version	Verwundbar bis	Fixversion (Ziel)
OBIEE 26.01	`26.01.0.0.0`	Patch CSPU Nov. 2026
OBIEE 8.2	`8.2.0.0.0`	Patch CSPU Nov. 2026

Angaben laut Oracle Critical Security Patch Update Advisory November 2026 (Produktfamilie Oracle Analytics). Oracle nennt nur die unterstützten Versionen; ältere, nicht mehr unterstützte Versionen sind **vermutlich ebenfalls betroffen** und erhalten keinen Patch. Oracle nennt **keinen Workaround**. Die passenden Patch-Nummern stehen im Patch Availability Document CPU451 in My Oracle Support.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf Systeme mit personenbezogenen Daten kann eine meldepflichtige Verletzung darstellen – DSGVO unverzüglich (i. d. R. 72 h), NIS-2 nach den für Sie geltenden Fristen. Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung und Dokumentation.

ZEITACHSE

17.11.2026
Oracle CSPU November 2026 · Patch verfügbar

17.11.2026
CVE im NVD veröffentlicht

15.12.2026
Nächster Oracle-Patchtermin (CSPU)

Stand heute
Nicht in CISA KEV · kein PoC

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

In dieser Reihenfolge – Erreichbarkeit vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
Erreichbarkeit einschränken	CSPU-Patch einspielen	Logs prüfen

01 Betroffenheit feststellen

Alle OBIEE-Installationen prüfen: `8.2.0.0.0` und `26.01.0.0.0` sind betroffen. Klären, ob OBIEE aus dem Internet oder aus Partnernetzen erreichbar ist.

02 Patchen

Den Patch aus dem Oracle Critical Security Patch Update November 2026 einspielen. Die Patch-Nummern je Version stehen im Patch Availability Document CPU451 in My Oracle Support. Vorher Konfiguration und Domänen sichern; Systeme auf nicht mehr unterstützten Versionen auf eine unterstützte Version heben.

03 Risiko bis zum Update senken

Oracle nennt keinen Workaround. OBIEE per Firewall oder VPN nur für interne Nutzer erreichbar machen und hinterlegte Zugangsdaten zu Datenquellen auf das nötige Minimum an Rechten prüfen.

04 Kompromittierung ausschließen

Zugriffs- und Server-Logs auf ungewöhnliche Anfragen, neue Administratorkonten, unerwartete Deployments und Konfigurationsänderungen prüfen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS

Keine – Oracle nennt keine, Ausnutzung nicht bekannt

AUSWERTUNGSQUELLEN

OBIEE- und WebLogic-Logs
Firewall- und Proxy-Logs
Abfrage-Logs der angebundenen Datenbanken

AUFFÄLLIGE MUSTER

Anfragen an OBIEE von unbekannten Adressen
ungewöhnliche Exporte, neue Benutzer oder Rollen

Zur Einordnung: Oracle veröffentlicht keine technischen Details. Die genannten Muster sind Ansatzpunkte für eine Auswertung, keine bestätigten Signaturen.

Wichtig: BI-Systeme bündeln Daten aus vielen Quellen und speichern die Zugänge dazu. Eine Übernahme öffnet damit oft mehr als nur die Berichte.

Bildmotive: KI-generierte Symbolbilder

Lassen Sie das von unseren Experten prüfen.

Drei Bausteine, die genau auf diese Schwachstelle einzahlen – vom schnellen Exposure-Check bis zur laufenden Absicherung.

Cyber Defense Center

24/7-SOC aus München: Eine HTTP-Anfrage an OBIEE von einer unbekannten Adresse, gefolgt von ungewöhnlichen Datenabfragen fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden Aus dem Internet erreichbare OBIEE-Instanzen über Ihren gesamten Perimeter – bevor Angreifer sie finden – und priorisieren nach realer Ausnutzung.

Incident-Response-Retainer

Bei Verdacht auf einen bereits erfolgten Zugriff übernimmt unser IR-Team Forensik und Eindämmung – mit vertraglich zugesicherter Reaktionszeit.

SO GEHEN WIR VOR

01 Exposure-Check

Wir prüfen, ob Ihre OBIEE-Systeme verwundbar konfiguriert und exponiert sind.

02 Sofortmaßnahmen begleiten

Mitigation und Patch-Fahrplan gemeinsam mit Ihrem Team umgesetzt.

03 Absichern & überwachen

Threat Hunting auf die IoCs, danach laufendes Monitoring und IR-Bereitschaft – 24/7, wenn Ihr Team das nicht selbst leisten kann.

Empfehlung für die Geschäftsleitung

- Einspielen des Oracle-Patches vom 17.11.2026 für OBIEE kurzfristig anordnen.
- Bestätigen lassen, dass die Systeme nicht offen im Internet stehen.
- Über eine dauerhafte Überwachung der Oracle-Middleware entscheiden.

Ihr Part · unser Part. Sie behalten die Kontrolle über Konfiguration und Freigaben; wir liefern Analyse, Bewertung und – im Retainer – die Reaktionskette.

Rollen, Eingriffstiefe und SLAs im Erstgespräch (RACI, AVV/TOM auf Anfrage) · Datenhaltung auf Wunsch vollständig in Deutschland · ISO/IEC 27001 (TÜV SÜD) · deutschsprachige Analysten.

Sprechen Sie mit uns, bevor es ein Angreifer tut.

Kostenloses 30-Minuten-Erstgespräch – wir prüfen Ihre Exposure gegenüber CVE-2026-114784 und dem OBIEE-Perimeter.

+49 89 45 24 24-100 · kontakt@argos.security · www.argos.security

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: Oracle Critical Security Patch Update Advisory November 2026 (17.11.2026, Risikomatrix Oracle Analytics, CVSS 10,0) · NVD (CVSS 3.1 Basiswert 10,0, Quelle Oracle als CNA) · CISA KEV (Stand 17.11.2026: nicht gelistet). Stand 17.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.