Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0502

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Oracle Analytics

Publicatiedatum: 18-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (NCSC) verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Oracle heeft meerdere kwetsbaarheden verholpen in Oracle Analytics en Business Intelligence Enterprise Edition (versies 8.2.0.0.0 tot en met 26.01.0.0.0) en aanverwante componenten zoals BI Publisher en Visual Analyzer.

Duiding

De kwetsbaarheden stellen een aanvaller in staat om via HTTP of SOAP-interface zonder of met lage privileges het systeem te compromitteren. Dit kan leiden tot volledige overname van het systeem, ongeautoriseerde toegang tot gevoelige data, wijziging of verwijdering van kritieke gegevens, en het veroorzaken van denial-of-service door het systeem te laten crashen of hangen. Sommige kwetsbaarheden vereisen gebruikersinteractie of infrastructuurtoegang, terwijl andere geen authenticatie vereisen. De impact betreft de vertrouwelijkheid, integriteit en beschikbaarheid van het systeem. Daarnaast zijn er kwetsbaarheden in de BI Publisher Web Service API die ongeautoriseerde leesrechten kunnen geven, en in de Visual Analyzer component die ongeautoriseerde datatoegang en -wijziging mogelijk maken. Ook zijn er gerelateerde Apache Log4j kwetsbaarheden die meerdere Oracle producten beïnvloeden, waaronder Oracle BI Enterprise Edition, welke kunnen leiden tot ongeautoriseerde datamodificatie en verstoring van logverwerking.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.oracle.com/security-alerts/cspunov2026.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-114784	10.0 CRITICAL
CVE-2026-114814	8.8 HIGH
CVE-2026-114783	8.6 HIGH
CVE-2026-114815	8.1 HIGH
CVE-2026-114817	8.1 HIGH
CVE-2026-114813	8.1 HIGH
CVE-2026-114793	7.8 HIGH
CVE-2026-114794	7.8 HIGH
CVE-2026-114790	6.8 MEDIUM
CVE-2026-114798	6.7 MEDIUM
CVE-2026-114801	6.7 MEDIUM
CVE-2026-114802	6.7 MEDIUM
CVE-2026-114804	6.5 MEDIUM
CVE-2026-114796	6.4 MEDIUM
CVE-2026-114803	6.4 MEDIUM
CVE-2026-114786	6.4 MEDIUM
CVE-2026-114797	6.1 MEDIUM
CVE-2026-114789	6.1 MEDIUM
CVE-2026-114800	6.1 MEDIUM
CVE-2026-49844	6.3 MEDIUM
CVE-2026-114810	5.5 MEDIUM
CVE-2026-114808	5.5 MEDIUM
CVE-2026-114787	5.4 MEDIUM
CVE-2026-114805	5.3 MEDIUM
CVE-2026-114811	4.3 MEDIUM
CVE-2026-114807	3.9 LOW
CVE-2026-114806	3.6 LOW

CWE's

CWE	Beschrijving
CWE-116	Improper Encoding or Escaping of Output

Getroffen producten

Oracle
Oracle BI Publisher
Oracle Business Intelligence Enterprise Edition

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions:
NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.