



Advisory NCSC-2026-0445

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Oracle Analytics

Publicatiedatum: 21-10-2026

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 delen. 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 33 kwetsbaarheden verholpen in diverse Oracle Analytics-producten, waaronder Oracle Business Intelligence Enterprise Edition en Oracle BI Publisher.

Duiding

In de patchnote staan 33 kwetsbaarheden, waarvan 14 kwetsbaarheden op afstand kunnen worden misbruikt zonder dat authenticatie vereist is. Afhankelijk van de kwetsbaarheid, de getroffen productversie en de configuratie kan misbruik leiden tot ongeautoriseerde toegang tot gevoelige gegevens, het aanmaken, wijzigen of verwijderen van gegevens, verstoring van de dienstverlening of compromittering van de getroffen component. De hoogst gerapporteerde CVSS 3.1-basiscore voor Oracle Analytics bedraagt 9,1 op een schaal van 10.

Oplossingen

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

Referenties

- <https://www.oracle.com/security-alerts/cpuoct2026.html>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-28387	8.1 HIGH
CVE-2026-31790	7.5 HIGH
CVE-2026-75803	9.8 CRITICAL
CVE-2026-87263	8.8 HIGH
CVE-2026-91241	9.1 CRITICAL
CVE-2026-91534	8.6 HIGH

CVE	CVSS Score
CVE-2026-91535	8.8 HIGH
CVE-2026-91539	7.8 HIGH
CVE-2026-91545	7.8 HIGH
CVE-2026-91546	8.1 HIGH
CVE-2026-91549	7.8 HIGH
CVE-2026-91557	7.0 HIGH
CVE-2026-91579	8.8 HIGH
CVE-2026-91597	8.3 HIGH
CVE-2026-91608	7.5 HIGH
CVE-2026-101531	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-354	Improper Validation of Integrity Check Value
CWE-416	Use After Free
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-824	Access of Uninitialized Pointer

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 or 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.