Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# NCSC-2026-0313

## Kwetsbaarheden verholpen in Oracle Business Intelligence Enterprise Edition en Oracle BI Publisher

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 19-08-2026

**TLP:WHITE**

**Toegestane verspreiding van TLP:WHITE**
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het 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.

Uw reacties zijn welkom op info@ncsc.nl

## Feiten

Oracle heeft meerdere kwetsbaarheden verholpen in Oracle Business Intelligence Enterprise Edition en Oracle BI Publisher.

## Duiding

De kwetsbaarheden bevinden zich in verschillende versies van Oracle Business Intelligence Enterprise Edition (versies 8.2.0.0.0, 12.2.1.4.0, en 26.01.0.0.0) en Oracle BI Publisher (versies 8.2.0.0.0, 12.2.1.4.0, en 26.01.0.0.0). Aanvallers met lage privileges en netwerktoegang via HTTP of SOAP kunnen hierdoor ongeautoriseerde toegang verkrijgen tot gevoelige data, authenticatiecontroles omzeilen, privileges escaleren, kritieke data wijzigen of verwijderen, en in sommige gevallen volledige controle over het systeem verkrijgen. Sommige kwetsbaarheden kunnen ook leiden tot gedeeltelijke denial-of-service condities. De kwetsbaarheden zijn aanwezig in componenten zoals de BI Search en de Web Service API van BI Publisher. De CVSS 3.1 basis scores variëren van 7.0 tot 9.9, wat duidt op een impact op vertrouwelijkheid, integriteit en beschikbaarheid van de systemen. Sommige aanvallen vereisen gebruikersinteractie of hogere privileges, terwijl andere ook door ongeauthenticeerde aanvallers kunnen worden misbruikt.

## Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden in Oracle Business Intelligence Enterprise Edition en BI Publisher te verhelpen. Zie bijgevoegde referenties voor meer informatie.

## Referenties

- https://www.oracle.com/security-alerts/cspuaug2026.html

## Kwetsbaarheden

| CVE | CVSS Score |
|---|---|
| CVE-2026-61302 | 8.2 HIGH |
| CVE-2026-61305 | 8.3 HIGH |
| CVE-2026-71055 | 8.8 HIGH |
| CVE-2026-71056 | 7.7 HIGH |
| CVE-2026-71057 | 8.5 HIGH |

| | |
|---|---|
| CVE-2026-71058 | 8.8 HIGH |
| CVE-2026-71059 | 9.9 CRITICAL |
| CVE-2026-71061 | 7.5 HIGH |
| CVE-2026-71094 | 7.3 HIGH |
| CVE-2026-71095 | 8.3 HIGH |
| CVE-2026-71096 | 8.2 HIGH |
| CVE-2026-71097 | 7.8 HIGH |
| CVE-2026-71098 | 7.0 HIGH |
| CVE-2026-71099 | 7.2 HIGH |
| CVE-2026-71107 | 7.5 HIGH |
| CVE-2026-71122 | 8.0 HIGH |

## CWE's

| CWE | Beschrijving |
|---|---|
| CWE-200 | Exposure of Sensitive Information to an Unauthorized Actor |

## Getroffen producten

| **Oracle** |
|---|
| Oracle BI Publisher |
| Oracle Business Intelligence Enterprise Edition |

## Disclaimer