



# NCSC-2026-0259

## Kwetsbaarheden verholpen in Oracle Analytics

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 22-07-2026

**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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

Oracle heeft meerdere kwetsbaarheden verholpen in Oracle BI Publisher (versies 8.2.0.0.0, 12.2.1.4.0 en 26.01.0.0.0) en Oracle Business Intelligence Enterprise Edition (versies 8.2.0.0.0 en 26.01.0.0.0).

## Duiding

De kwetsbaarheden in Oracle BI Publisher en Oracle Business Intelligence Enterprise Edition stellen ongeauthenticeerde aanvallers in staat via HTTP-verzoeken volledige systeemcompromittering te bereiken, authenticatie te omzeilen, willekeurige code uit te voeren, denial of service aanvallen uit te voeren en ongeautoriseerde lees-, update-, insert- of delete-operaties op onderliggende data uit te voeren. Daarnaast kunnen laaggeprivilegieerde aanvallers via de Web Service API authenticatiecontroles omzeilen, wat leidt tot ongeautoriseerde toegang tot gevoelige data, wijziging of verwijdering van kritieke informatie en gedeeltelijke denial of service condities.

## Oplossingen

Apache heeft een fix uitgebracht in Apache Log4j versie 2.25.4. Oracle heeft updates uitgebracht voor Oracle BI Publisher en Oracle Business Intelligence Enterprise Edition om de beschreven kwetsbaarheden te verhelpen. Daarnaast is de buffer overflow in de cryptography package opgelost in versie 46.0.7. Zie bijgevoegde referenties voor meer informatie.

## Referenties

- <https://www.oracle.com/security-alerts/cpujul2026.html>
- <https://www.oracle.com/security-alerts/cpujul2026verbose.html>

## Kwetsbaarheden

| CVE                              | CVSS Score   |
|----------------------------------|--------------|
| ➤ <a href="#">CVE-2026-34480</a> | 6.9 MEDIUM   |
| ➤ <a href="#">CVE-2026-39892</a> | 6.9 MEDIUM   |
| ➤ <a href="#">CVE-2026-60173</a> | 9.8 CRITICAL |
| ➤ <a href="#">CVE-2026-60671</a> | 8.6 HIGH     |
| ➤ <a href="#">CVE-2026-60673</a> | 6.5 MEDIUM   |

[> CVE-2026-60674](#)

8.2 HIGH

[> CVE-2026-60719](#)

9.9 CRITICAL

## CWE's

| CWE                          | Beschrijving                                                            |
|------------------------------|-------------------------------------------------------------------------|
| <a href="#">&gt; CWE-116</a> | Improper Encoding or Escaping of Output                                 |
| <a href="#">&gt; CWE-119</a> | Improper Restriction of Operations within the Bounds of a Memory Buffer |
| <a href="#">&gt; CWE-131</a> | Incorrect Calculation of Buffer Size                                    |
| <a href="#">&gt; CWE-168</a> | Improper Handling of Inconsistent Special Elements                      |

## Getroffen producten

|                                                    |
|----------------------------------------------------|
| <b>Oracle</b>                                      |
| Oracle BI<br>Publisher                             |
| Oracle Business Intelligence<br>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.