Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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).

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 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
CVE-2026-34480	6.9 MEDIUM
CVE-2026-39892	6.9 MEDIUM
CVE-2026-60173	9.8 CRITICAL
CVE-2026-60671	8.6 HIGH
CVE-2026-60673	6.5 MEDIUM

CVE-2026-60674	8.2 HIGH
CVE-2026-60719	9.9 CRITICAL

CWE's

CWE	Beschrijving
CWE-116	Improper Encoding or Escaping of Output
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-131	Incorrect Calculation of Buffer Size
CWE-168	Improper Handling of Inconsistent Special Elements

Getroffen producten

Oracle
Oracle BI Publisher
Oracle Business Intelligence Enterprise Edition

Disclaimer