



NCSC-2025-0028

Kwetsbaarheden verholpen in Oracle Analytics

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 22-01-2025

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 kwetsbaarheden verholpen in Oracle Analytics producten, zoals Business Intelligence, Analytics Desktop en BI Publisher.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om een Denial-of-Service te veroorzaken, of zich toegang te verschaffen tot gevoelige gegevens.

Oplossingen

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

Referenties

➤ <https://www.oracle.com/security-alerts/cpujan2025.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2016-10000	
➤ CVE-2020-2849	
➤ CVE-2020-7760	7.5 HIGH
➤ CVE-2020-13956	5.3 MEDIUM
➤ CVE-2020-28975	7.5 HIGH
➤ CVE-2021-23926	9.1 CRITICAL
➤ CVE-2021-33813	7.5 HIGH
➤ CVE-2022-40150	7.5 HIGH
➤ CVE-2023-2976	7.5 HIGH

> CVE-2023-4785	
> CVE-2023-7272	8.6 HIGH
> CVE-2023-24998	
> CVE-2023-25399	9.8 CRITICAL
> CVE-2023-29824	9.8 CRITICAL
> CVE-2023-32732	7.5 HIGH
> CVE-2023-33202	7.5 HIGH
> CVE-2023-33953	7.5 HIGH
> CVE-2023-43804	8.1 HIGH
> CVE-2023-44487	7.5 HIGH
> CVE-2023-45803	4.4 MEDIUM
> CVE-2023-50782	7.5 HIGH
> CVE-2024-0727	7.5 HIGH
> CVE-2024-1135	8.2 HIGH
> CVE-2024-4741	
> CVE-2024-5535	9.1 CRITICAL
> CVE-2024-7254	8.2 HIGH
> CVE-2024-22195	6.1 MEDIUM
> CVE-2024-26130	7.5 HIGH
> CVE-2024-29025	7.3 HIGH
> CVE-2024-29131	8.1 HIGH
> CVE-2024-34064	5.4 MEDIUM
> CVE-2024-35195	5.7 MEDIUM

> CVE-2024-36114	8.6 HIGH
> CVE-2024-37891	4.4 MEDIUM
> CVE-2024-38809	8.0 HIGH
> CVE-2024-38820	9.8 CRITICAL
> CVE-2024-43382	5.9 MEDIUM
> CVE-2024-47561	9.8 CRITICAL
> CVE-2025-21532	7.8 HIGH

CWE's

CWE	Beschrijving
> CVE-416	Use After Free
> CVE-476	NULL Pointer Dereference
> CVE-400	Uncontrolled Resource Consumption
> CVE-770	Allocation of Resources Without Limits or Throttling
> CVE-502	Deserialization of Untrusted Data
> CVE-248	Uncaught Exception
> CVE-674	Uncontrolled Recursion
> CVE-611	Improper Restriction of XML External Entity Reference
> CVE-787	Out-of-bounds Write
> CVE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CVE-789	Memory Allocation with Excessive Size Value
> CVE-20	Improper Input Validation
> CVE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> CVE-1395	Dependency on Vulnerable Third-Party Component

➤ CWE-670	Always-Incorrect Control Flow Implementation
➤ CWE-399	CWE-399
➤ CWE-326	Inadequate Encryption Strength
➤ CWE-669	Incorrect Resource Transfer Between Spheres
➤ CWE-776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')
➤ CWE-834	Excessive Iteration
➤ CWE-311	Missing Encryption of Sensitive Data
➤ CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
➤ CWE-125	Out-of-bounds Read
➤ CWE-404	Improper Resource Shutdown or Release
➤ CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
➤ CWE-1333	Inefficient Regular Expression Complexity

Getroffen producten

oracle
business_intelligence
business_intelligence_enterprise_edition
bi_publisher
analytics_desktop

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.