Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0129

Kwetsbaarheden verholpen in Oracle Analytics

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 16-04-2025

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.

Duiding

De kwetsbaarheden stellen ongeauthenticeerde kwaadwillenden in staat om toegang te krijgen tot gevoelige gegevens, Denial-of-Service aan te richten, en zelfs volledige controle over systemen te verkrijgen. Specifieke kwetsbaarheden in Oracle Business Intelligence Enterprise Edition kunnen leiden tot ongeautoriseerde toegang en manipulatie van gegevens via HTTP. Daarnaast zijn er kwetsbaarheden die Denial-of-Service kunnen veroorzaken door onjuiste invoer of misbruik van systeemfunctionaliteiten.

Oplossingen

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

Referenties

- https://www.oracle.com/security-alerts/cpuapr2025.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2022-36033	8.8 HIGH
CVE-2023-24998	
CVE-2023-25399	9.8 CRITICAL
CVE-2023-38546	9.8 CRITICAL
CVE-2023-52428	8.7 HIGH
CVE-2024-7264	5.1 MEDIUM
CVE-2024-9143	6.9 MEDIUM
CVE-2024-30172	6.9 MEDIUM

CVE-2024-32007	6.9 MEDIUM
CVE-2024-37891	4.4 MEDIUM
CVE-2024-38820	2.3 LOW
CVE-2024-38827	6.3 MEDIUM
CVE-2024-52046	10.0 CRITICAL
CVE-2025-30723	5.4 MEDIUM
CVE-2025-30724	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-399	CWE-399
CWE-669	Incorrect Resource Transfer Between Spheres
CWE-178	Improper Handling of Case Sensitivity
CWE-311	Missing Encryption of Sensitive Data
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-125	Out-of-bounds Read
CWE-404	Improper Resource Shutdown or Release
CWE-284	Improper Access Control
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-400	Uncontrolled Resource Consumption
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-502	Deserialization of Untrusted Data
CWE-787	Out-of-bounds Write
CWE-73	External Control of File Name or Path

CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
CWE-20	Improper Input Validation
CWE-87	Improper Neutralization of Alternate XSS Syntax
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

Oracle
Oracle Business Intelligence Enterprise Edition
Oracle BI Publisher
BI Publisher
Oracle Corporation
Oracle BI Publisher

Disclaimer