Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0123

Kwetsbaarheden verholpen in Oracle Database Producten

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 diverse Oracle Database Producten en subsystemen, zoals Oracle Server, NoSQL, TimesTen, Secure Backup en Essbase.

Duiding

De kwetsbaarheden stellen ongeauthenticeerde kwaadwillenden in staat om een Denial-of-Service te veroorzaken of om ongeautoriseerde toegang te verkrijgen tot gevoelige gegevens en gegevens te manipuleren. Subcomponenten als de RDBMS Listener, Java VM, en andere componenten zijn specifiek kwetsbaar, met CVSS-scores variërend van 5.3 tot 7.5, wat duidt op een gematigd tot hoog risico.

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-2020-1935	7.5 HIGH
CVE-2020-1938	9.8 CRITICAL
CVE-2020-9484	7.5 HIGH
CVE-2020-11996	
CVE-2020-13935	
CVE-2020-13943	7.5 HIGH
CVE-2020-36843	2.0 LOW
CVE-2021-24122	7.5 HIGH

CVE-2021-25122	7.5 HIGH
CVE-2021-25329	7.5 HIGH
CVE-2021-30640	7.5 HIGH
CVE-2021-33037	7.5 HIGH
CVE-2021-41079	7.5 HIGH
CVE-2021-41184	6.5 MEDIUM
CVE-2021-42575	
CVE-2021-43980	7.5 HIGH
CVE-2022-3786	9.8 CRITICAL
CVE-2022-25762	8.6 HIGH
CVE-2022-42252	7.5 HIGH
CVE-2023-28708	7.5 HIGH
CVE-2023-34053	7.5 HIGH
CVE-2023-41080	7.5 HIGH
CVE-2023-42795	7.5 HIGH
CVE-2023-44487	6.9 MEDIUM
CVE-2023-45648	7.5 HIGH
CVE-2023-46589	7.5 HIGH
CVE-2024-6763	
CVE-2024-8176	5.1 MEDIUM
CVE-2024-8184	6.5 MEDIUM
CVE-2024-9143	6.9 MEDIUM
CVE-2024-11053	9.1 CRITICAL

CVE-2024-11233	6.3 MEDIUM
CVE-2024-11234	6.3 MEDIUM
CVE-2024-11236	9.3 CRITICAL
CVE-2024-13176	5.9 MEDIUM
CVE-2024-23672	7.5 HIGH
CVE-2024-24549	6.6 MEDIUM
CVE-2024-36114	8.6 HIGH
CVE-2024-37891	4.4 MEDIUM
CVE-2024-38819	6.9 MEDIUM
CVE-2024-38820	2.3 LOW
CVE-2024-38999	8.9 HIGH
CVE-2024-39338	5.1 MEDIUM
CVE-2024-47554	8.7 HIGH
CVE-2024-47561	9.3 CRITICAL
CVE-2024-53382	2.3 LOW
CVE-2024-57699	5.1 MEDIUM
CVE-2025-21578	6.7 MEDIUM
CVE-2025-24813	9.2 CRITICAL
CVE-2025-24970	6.9 MEDIUM
CVE-2025-25193	4.8 MEDIUM
CVE-2025-26791	4.5 MEDIUM
CVE-2025-30694	5.4 MEDIUM
CVE-2025-30701	7.3 HIGH

CVE-2025-30702	**5.3 MEDIUM**
CVE-2025-30733	**6.5 MEDIUM**
CVE-2025-30736	**7.4 HIGH**

CWE's

CWE	Beschrijving
CWE-385	Covert Timing Channel
CWE-347	Improper Verification of Cryptographic Signature
CWE-1286	Improper Validation of Syntactic Correctness of Input
CWE-125	Out-of-bounds Read
CWE-404	Improper Resource Shutdown or Release
CWE-400	Uncontrolled Resource Consumption
CWE-502	Deserialization of Untrusted Data
CWE-918	Server-Side Request Forgery (SSRF)
CWE-787	Out-of-bounds Write
CWE-20	Improper Input Validation
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-44	Path Equivalence: 'file.name' (Internal Dot)
CWE-226	Sensitive Information in Resource Not Removed Before Reuse
CWE-706	Use of Incorrectly-Resolved Name or Reference
CWE-669	Incorrect Resource Transfer Between Spheres
CWE-755	Improper Handling of Exceptional Conditions
CWE-178	Improper Handling of Case Sensitivity
CWE-193	Off-by-one Error
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')

CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
CWE-523	Unprotected Transport of Credentials
CWE-190	Integer Overflow or Wraparound
CWE-614	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute
CWE-285	Improper Authorization
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-284	Improper Access Control
CWE-1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
CWE-476	NULL Pointer Dereference
CWE-459	Incomplete Cleanup
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
CWE-674	Uncontrolled Recursion
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-122	Heap-based Buffer Overflow
CWE-121	Stack-based Buffer Overflow
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-269	Improper Privilege Management
CWE-287	Improper Authentication

Getroffen producten

Oracle
Database Server
Enterprise Manager for Oracle Database
GoldenGate
Big Data Spatial and Graph
Oracle Database Server
Oracle Enterprise Manager for Oracle Database
Oracle NoSQL Database
Oracle TimesTen In-Memory Database
Autonomous Health Framework
Oracle Essbase
GoldenGate Stream Analytics
Oracle GoldenGate
Oracle GoldenGate Big Data and Application Adapters
Oracle GoldenGate Stream Analytics
Graph Server and Client

Oracle Big Data Spatial and Graph
Oracle Secure Backup
Oracle Corporation
Oracle Database Server
Oracle Secure Backup

Disclaimer