Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0020

Kwetsbaarheden verholpen in Oracle Database producten

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 diverse database producten en subsystemen, zoals de Core Database, Graal, Application Express, GoldenGate en REST data.

Duiding

De kwetsbaarheden bevinden zich in verschillende componenten van de Oracle Database, waaronder de Data Mining component en de Java VM. Deze kwetsbaarheden stellen laaggeprivilegieerde geauthenticeerde gebruikers in staat om het systeem te compromitteren, wat kan leiden tot ongeautoriseerde toegang en gegevensmanipulatie. De Java VM-kwetsbaarheid kan ook leiden tot ongeautoriseerde wijzigingen van 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-2024-38998	9.8 CRITICAL
CVE-2024-38999	10.0 CRITICAL
CVE-2024-45490	
CVE-2024-45491	
CVE-2024-45492	
CVE-2024-45772	
CVE-2024-47554	
CVE-2024-47561	9.8 CRITICAL

CVE-2024-50379	
CVE-2024-52316	
CVE-2024-54677	
CVE-2024-56337	
CVE-2025-21553	
CVE-2025-21557	5.4 MEDIUM
CVE-2022-26345	6.7 MEDIUM
CVE-2023-27043	
CVE-2023-36730	7.8 HIGH
CVE-2023-36785	7.8 HIGH
CVE-2023-48795	7.5 HIGH
CVE-2023-52428	7.5 HIGH
CVE-2024-2961	8.8 HIGH
CVE-2024-4030	
CVE-2024-4032	
CVE-2024-6232	
CVE-2024-6763	5.3 MEDIUM
CVE-2024-6923	
CVE-2024-7254	
CVE-2024-7592	
CVE-2024-8088	
CVE-2024-8927	7.5 HIGH
CVE-2024-11053	

CVE-2024-21211	3.7 LOW
CVE-2024-22262	8.1 HIGH
CVE-2024-24789	
CVE-2024-24790	
CVE-2024-24791	
CVE-2024-28757	7.5 HIGH
CVE-2024-33599	
CVE-2024-33600	
CVE-2024-33601	
CVE-2024-33602	
CVE-2024-38819	7.5 HIGH
CVE-2024-38820	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-391	Unchecked Error Condition
CWE-115	Misinterpretation of Input
CWE-466	Return of Pointer Value Outside of Expected Range
CWE-222	Truncation of Security-relevant Information
CWE-131	Incorrect Calculation of Buffer Size
CWE-1287	Improper Validation of Specified Type of Input
CWE-922	Insecure Storage of Sensitive Information
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-1220	Insufficient Granularity of Access Control

CWE-776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')
CWE-178	Improper Handling of Case Sensitivity
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-440	Expected Behavior Violation
CWE-1286	Improper Validation of Syntactic Correctness of Input
CWE-703	Improper Check or Handling of Exceptional Conditions
CWE-617	Reachable Assertion
CWE-427	Uncontrolled Search Path Element
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-354	Improper Validation of Integrity Check Value
CWE-190	Integer Overflow or Wraparound
CWE-404	Improper Resource Shutdown or Release
CWE-284	Improper Access Control
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-1333	Inefficient Regular Expression Complexity
CWE-1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
CWE-476	NULL Pointer Dereference
CWE-757	Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade')
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-674	Uncontrolled Recursion

CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-611	Improper Restriction of XML External Entity Reference
CWE-787	Out-of-bounds Write
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-122	Heap-based Buffer Overflow
CWE-121	Stack-based Buffer Overflow
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
CWE-20	Improper Input Validation
CWE-276	Incorrect Default Permissions

Getroffen producten

oracle
graal_development_kit_for_micronaut
database_- _data_mining
database_migration_assistant_for_unicode
database_server
database_- _graalvm_multilingual_engine
application_express
goldengate
goldengate_big_data_and_application_adapters
rest_data_services
secure_backup

Disclaimer