Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0411

Kwetsbaarheden verholpen in Oracle Database producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 17-10-2024

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, Application Express, Autonomous Health Framework, Essbase, GoldenGate, SQL Developer en Secure Backup.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial-of-Service (DoS)
- Manipuleren van data
- Toegang 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/cpuoct2024.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2022-1471	
CVE-2022-34169	7.5 HIGH
CVE-2022-36033	8.8 HIGH
CVE-2022-37454	9.8 CRITICAL
CVE-2022-38136	
CVE-2022-40196	
CVE-2022-41342	

CVE-2022-42919	
CVE-2022-45061	7.5 HIGH
CVE-2022-46337	9.8 CRITICAL
CVE-2023-2976	7.1 HIGH
CVE-2023-4043	7.5 HIGH
CVE-2023-4759	8.8 HIGH
CVE-2023-4863	
CVE-2023-5072	7.5 HIGH
CVE-2023-26031	7.5 HIGH
CVE-2023-26551	0.0 NONE
CVE-2023-26552	5.6 MEDIUM
CVE-2023-26553	5.6 MEDIUM
CVE-2023-26554	5.6 MEDIUM
CVE-2023-26555	6.4 MEDIUM
CVE-2023-28484	6.5 MEDIUM
CVE-2023-29469	6.5 MEDIUM
CVE-2023-33201	5.3 MEDIUM
CVE-2023-37920	9.8 CRITICAL
CVE-2023-39410	7.5 HIGH
CVE-2023-44487	7.5 HIGH
CVE-2023-44981	9.1 CRITICAL
CVE-2023-45288	7.5 HIGH
CVE-2023-48795	5.9 MEDIUM

CVE-2023-49083	7.5 HIGH
CVE-2023-51384	5.9 MEDIUM
CVE-2023-51385	6.5 MEDIUM
CVE-2023-52425	7.5 HIGH
CVE-2023-52426	7.5 HIGH
CVE-2024-1874	9.8 CRITICAL
CVE-2024-2408	9.8 CRITICAL
CVE-2024-2511	7.5 HIGH
CVE-2024-4577	9.8 CRITICAL
CVE-2024-4603	7.5 HIGH
CVE-2024-4741	7.5 HIGH
CVE-2024-5458	9.8 CRITICAL
CVE-2024-5535	9.1 CRITICAL
CVE-2024-5585	9.8 CRITICAL
CVE-2024-6119	9.1 CRITICAL
CVE-2024-6232	
CVE-2024-7264	6.5 MEDIUM
CVE-2024-7592	
CVE-2024-21131	
CVE-2024-21138	
CVE-2024-21140	
CVE-2024-21144	
CVE-2024-21145	

CVE-2024-21147	
CVE-2024-21233	4.3 MEDIUM
CVE-2024-21242	3.5 LOW
CVE-2024-21251	3.1 LOW
CVE-2024-21261	4.9 MEDIUM
CVE-2024-22018	7.1 HIGH
CVE-2024-22020	8.1 HIGH
CVE-2024-22201	7.5 HIGH
CVE-2024-23807	8.1 HIGH
CVE-2024-23944	5.3 MEDIUM
CVE-2024-24989	
CVE-2024-24990	7.5 HIGH
CVE-2024-25710	8.1 HIGH
CVE-2024-26130	7.5 HIGH
CVE-2024-26308	5.9 MEDIUM
CVE-2024-27983	8.2 HIGH
CVE-2024-28182	7.5 HIGH
CVE-2024-28849	6.5 MEDIUM
CVE-2024-28887	7.8 HIGH
CVE-2024-29025	7.3 HIGH
CVE-2024-29131	7.3 HIGH
CVE-2024-29133	7.3 HIGH
CVE-2024-31079	6.5 MEDIUM

CVE-2024-32760	7.5 HIGH
CVE-2024-34161	6.5 MEDIUM
CVE-2024-34750	7.5 HIGH
CVE-2024-35200	7.5 HIGH
CVE-2024-36137	7.1 HIGH
CVE-2024-36138	
CVE-2024-36387	7.5 HIGH
CVE-2024-37370	9.1 CRITICAL
CVE-2024-37371	9.1 CRITICAL
CVE-2024-37372	7.1 HIGH
CVE-2024-38356	6.1 MEDIUM
CVE-2024-38357	6.1 MEDIUM
CVE-2024-38472	7.5 HIGH
CVE-2024-38473	8.1 HIGH
CVE-2024-38474	9.8 CRITICAL
CVE-2024-38475	9.1 CRITICAL
CVE-2024-38476	9.8 CRITICAL
CVE-2024-38477	7.5 HIGH
CVE-2024-38998	9.8 CRITICAL
CVE-2024-38999	10.0 CRITICAL
CVE-2024-39573	7.5 HIGH
CVE-2024-39884	7.5 HIGH
CVE-2024-40725	7.5 HIGH

CVE-2024-40898	7.5 HIGH
CVE-2024-45490	9.8 CRITICAL
CVE-2024-45491	9.8 CRITICAL
CVE-2024-45492	9.8 CRITICAL
CVE-2024-45801	7.3 HIGH

CWE's

CWE	Beschrijving
CWE-130	Improper Handling of Length Parameter Inconsistency
CWE-208	Observable Timing Discrepancy
CWE-776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')
CWE-88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')
CWE-755	Improper Handling of Exceptional Conditions
CWE-834	Excessive Iteration
CWE-407	Inefficient Algorithmic Complexity
CWE-178	Improper Handling of Case Sensitivity
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-415	Double Free
CWE-311	Missing Encryption of Sensitive Data
CWE-427	Uncontrolled Search Path Element
CWE-172	Encoding Error
CWE-680	Integer Overflow to Buffer Overflow
CWE-426	Untrusted Search Path
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')

CWE-116	Improper Encoding or Escaping of Output
CWE-345	Insufficient Verification of Data Authenticity
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-203	Observable Discrepancy
CWE-190	Integer Overflow or Wraparound
CWE-552	Files or Directories Accessible to External Parties
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-125	Out-of-bounds Read
CWE-404	Improper Resource Shutdown or Release
CWE-275	CWE-275
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-416	Use After Free
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-476	NULL Pointer Dereference
CWE-295	Improper Certificate Validation
CWE-668	Exposure of Resource to Wrong Sphere
CWE-829	Inclusion of Functionality from Untrusted Control Sphere
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-400	Uncontrolled Resource Consumption
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-502	Deserialization of Untrusted Data
CWE-918	Server-Side Request Forgery (SSRF)

CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
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-681	Incorrect Conversion between Numeric Types
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
CWE-269	Improper Privilege Management
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')
CWE-18	CWE-18
CWE-385	Covert Timing Channel
CWE-606	Unchecked Input for Loop Condition
CWE-192	Integer Coercion Error
CWE-390	Detection of Error Condition Without Action
CWE-1325	Improperly Controlled Sequential Memory Allocation
CWE-222	Truncation of Security-relevant Information
CWE-131	Incorrect Calculation of Buffer Size
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-304	Missing Critical Step in Authentication

Getroffen producten

oracle
database_- _grid
database_- _core
database_- _security
spatial_and_graph_mapviewer
spatial_and_graph
fleet_patching_and_provisioning_- _micronaut
fleet_patching_and_provisioning
database_- _xml_database
database_- _java_vm
autonomous_health_framework
graalvm_for_jdk
sqlcl
application_express_administration
application_express_customers_plugin
application_express_team_calendar_plugin
application_express
blockchain_platform
essbase
oracle_essbase

goldengate_big_data_and_application_adapters
goldengate_big_data
goldengate_stream_analytics
goldengate_studio
goldengate_veridata
goldengate
oracle_goldengate_stream_analytics
management_pack_for__goldengate
oracle_goldengate_studio
oracle_goldengate
nosql_database
oracle_nosql_database
oracle_secure_backup
secure_backup
oracle_sql_developer
sql_developer
oracle_corporation
oracle_application_express

Disclaimer