Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0303

Kwetsbaarheden verholpen in Oracle MySQL

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 17-07-2024

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

Er zijn kwetsbaarheden verholpen in Oracle MySQL.

Duiding

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

- Denial-of-Service (DoS)
- Toegang tot gevoelige gegevens
- Toegang tot systeemgegevens
- Manipulatie van gegevens
- (Remote) code execution (Gebruikersrechten)

Oplossingen

Oracle heeft updates beschikbaar gesteld om de kwetsbaarheden te verhelpen. Zie de referenties voor meer informatie.

Referenties

- https://nvd.nist.gov/vuln/detail/CVE-2021-24112
- https://nvd.nist.gov/vuln/detail/CVE-2023-37920
- https://nvd.nist.gov/vuln/detail/CVE-2023-48795
- https://nvd.nist.gov/vuln/detail/CVE-2023-52425
- https://nvd.nist.gov/vuln/detail/CVE-2023-6129
- https://nvd.nist.gov/vuln/detail/CVE-2024-0450
- https://nvd.nist.gov/vuln/detail/CVE-2024-20996
- https://nvd.nist.gov/vuln/detail/CVE-2024-21125
- https://nvd.nist.gov/vuln/detail/CVE-2024-21127
- https://nvd.nist.gov/vuln/detail/CVE-2024-21129
- https://nvd.nist.gov/vuln/detail/CVE-2024-21130
- https://nvd.nist.gov/vuln/detail/CVE-2024-21134
- https://nvd.nist.gov/vuln/detail/CVE-2024-21135
- https://nvd.nist.gov/vuln/detail/CVE-2024-21137
- https://nvd.nist.gov/vuln/detail/CVE-2024-21142
- https://nvd.nist.gov/vuln/detail/CVE-2024-21157
- https://nvd.nist.gov/vuln/detail/CVE-2024-21159
- https://nvd.nist.gov/vuln/detail/CVE-2024-21160

- https://nvd.nist.gov/vuln/detail/CVE-2024-21162
- https://nvd.nist.gov/vuln/detail/CVE-2024-21163
- https://nvd.nist.gov/vuln/detail/CVE-2024-21165
- https://nvd.nist.gov/vuln/detail/CVE-2024-21166
- https://nvd.nist.gov/vuln/detail/CVE-2024-21170
- https://nvd.nist.gov/vuln/detail/CVE-2024-21171
- https://nvd.nist.gov/vuln/detail/CVE-2024-21173
- https://nvd.nist.gov/vuln/detail/CVE-2024-21176
- https://nvd.nist.gov/vuln/detail/CVE-2024-21177
- https://nvd.nist.gov/vuln/detail/CVE-2024-21179
- https://nvd.nist.gov/vuln/detail/CVE-2024-21185
- https://nvd.nist.gov/vuln/detail/CVE-2024-22257
- https://nvd.nist.gov/vuln/detail/CVE-2024-22262
- https://nvd.nist.gov/vuln/detail/CVE-2024-24549
- https://nvd.nist.gov/vuln/detail/CVE-2024-25062
- https://www.oracle.com/docs/tech/security-alerts/cpujul2024csaf.json
- https://www.oracle.com/security-alerts/cpujul2024.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2021-24112	
CVE-2023-6129	6.5 MEDIUM
CVE-2023-37920	9.8 CRITICAL
CVE-2023-48795	5.9 MEDIUM
CVE-2023-52425	7.5 HIGH
CVE-2024-0450	6.2 MEDIUM
CVE-2024-20996	4.9 MEDIUM
CVE-2024-21125	4.9 MEDIUM
CVE-2024-21127	4.9 MEDIUM
CVE-2024-21129	4.9 MEDIUM

CVE-2024-21130	4.9 MEDIUM
CVE-2024-21134	4.3 MEDIUM
CVE-2024-21135	4.9 MEDIUM
CVE-2024-21137	4.9 MEDIUM
CVE-2024-21142	4.9 MEDIUM
CVE-2024-21157	4.9 MEDIUM
CVE-2024-21159	4.9 MEDIUM
CVE-2024-21160	4.9 MEDIUM
CVE-2024-21162	4.9 MEDIUM
CVE-2024-21163	5.5 MEDIUM
CVE-2024-21165	4.9 MEDIUM
CVE-2024-21166	5.9 MEDIUM
CVE-2024-21170	6.3 MEDIUM
CVE-2024-21171	6.5 MEDIUM
CVE-2024-21173	4.9 MEDIUM
CVE-2024-21176	5.3 MEDIUM
CVE-2024-21177	6.5 MEDIUM
CVE-2024-21179	4.9 MEDIUM
CVE-2024-21185	4.9 MEDIUM
CVE-2024-22257	8.2 HIGH
CVE-2024-22262	8.1 HIGH
CVE-2024-24549	7.5 HIGH
CVE-2024-25062	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-222	Truncation of Security-relevant Information
CWE-284	Improper Access Control
CWE-285	Improper Authorization
CWE-295	Improper Certificate Validation
CWE-328	Use of Weak Hash
CWE-345	Insufficient Verification of Data Authenticity
CWE-400	Uncontrolled Resource Consumption
CWE-404	Improper Resource Shutdown or Release
CWE-405	Asymmetric Resource Consumption (Amplification)
CWE-416	Use After Free
CWE-450	Multiple Interpretations of UI Input
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')

Getroffen producten

oracle
mysql_cluster
mysql_connectors
mysql_enterprise_backup
mysql_enterprise_monitor
mysql_ndb_cluster
mysql_server
mysql_workbench

mysql

Disclaimer