Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0262

Kwetsbaarheden verholpen in Oracle MySQL Server en MySQL Cluster

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 22-07-2026

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 meerdere kwetsbaarheden verholpen in Oracle MySQL Server en MySQL Cluster.

Duiding

De kwetsbaarheden betreffen verschillende versies van Oracle MySQL Server en MySQL Cluster. Een aantal kwetsbaarheden stelt een aanvaller met hoge privileges en netwerktoegang in staat om een denial-of-service (DoS) te veroorzaken, waarbij de server kan hangen of crashen, wat de beschikbaarheid van de database beïnvloedt. Sommige DoS-kwetsbaarheden kunnen ook door laaggeprivilegieerde gebruikers worden misbruikt.

Daarnaast zijn er kwetsbaarheden in de Group Replication Plugin en de NDB Operator component die DoS of ongeautoriseerde toegang tot data mogelijk maken.

Verder zijn er kwetsbaarheden die een aanvaller met hoge privileges en netwerktoegang in staat stellen om volledige controle over de server te verkrijgen, wat impact heeft op vertrouwelijkheid, integriteit en beschikbaarheid.

Ook zijn er kwetsbaarheden in Oracle MySQL Connectors (Connector/C++, Connector/Net, Connector/J) die ongeauthenticeerde of laaggeprivilegieerde aanvallers met netwerktoegang toestaan om data te manipuleren, toegang te verkrijgen tot gevoelige informatie of een denial-of-service te veroorzaken. Sommige kwetsbaarheden vereisen gebruikersinteractie of lokale toegang.

De CVSS 3.1 scores variëren van laag (2.2) tot hoog (8.5), afhankelijk van het type kwetsbaarheid en de impact op de systemen. De kwetsbaarheden zijn specifiek voor Oracle MySQL Server, MySQL Cluster en de MySQL Connectors, en zijn exploiteerbaar via netwerktoegang, soms met aanvullende vereisten zoals infrastructuurtoegang, gebruikersinteractie of lokale toegang.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden in Oracle MySQL Server, MySQL Cluster en MySQL Connectors te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.oracle.com/security-alerts/cpujul2026.html
- https://www.oracle.com/security-alerts/cpujul2026verbose.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-46936	4.4 MEDIUM
CVE-2026-47008	4.9 MEDIUM
CVE-2026-47012	4.4 MEDIUM
CVE-2026-47023	4.9 MEDIUM
CVE-2026-47052	6.9 MEDIUM
CVE-2026-47064	6.5 MEDIUM
CVE-2026-60145	4.9 MEDIUM
CVE-2026-60163	8.4 HIGH
CVE-2026-60171	4.9 MEDIUM
CVE-2026-60174	6.5 MEDIUM
CVE-2026-60177	4.4 MEDIUM
CVE-2026-60178	6.6 MEDIUM
CVE-2026-60179	7.4 HIGH
CVE-2026-60180	7.5 HIGH
CVE-2026-60181	6.7 MEDIUM
CVE-2026-60182	4.4 MEDIUM
CVE-2026-60183	6.4 MEDIUM
CVE-2026-60184	4.4 MEDIUM
CVE-2026-60185	4.4 MEDIUM
CVE-2026-60186	4.4 MEDIUM
CVE-2026-60187	4.4 MEDIUM
CVE-2026-60188	4.4 MEDIUM

CVE-2026-60189	4.4 MEDIUM
CVE-2026-60190	2.2 LOW
CVE-2026-60191	4.1 MEDIUM
CVE-2026-60192	8.1 HIGH
CVE-2026-60193	8.5 HIGH
CVE-2026-60194	4.9 MEDIUM
CVE-2026-60195	4.9 MEDIUM
CVE-2026-60311	6.5 MEDIUM
CVE-2026-60314	7.5 HIGH
CVE-2026-60315	8.2 HIGH
CVE-2026-60316	7.2 HIGH
CVE-2026-60317	7.4 HIGH
CVE-2026-60324	6.5 MEDIUM
CVE-2026-60331	6.4 MEDIUM
CVE-2026-60332	6.4 MEDIUM
CVE-2026-60569	5.1 MEDIUM
CVE-2026-60585	6.6 MEDIUM
CVE-2026-60586	7.7 HIGH
CVE-2026-60623	7.1 HIGH
CVE-2026-60624	6.5 MEDIUM
CVE-2026-60718	6.5 MEDIUM
CVE-2026-60725	7.4 HIGH
CVE-2026-60747	6.2 MEDIUM

CVE-2026-61081	2.7 LOW
CVE-2026-61082	6.5 MEDIUM
CVE-2026-61093	6.5 MEDIUM
CVE-2026-61094	7.2 HIGH
CVE-2026-61096	2.9 LOW
CVE-2026-61108	6.5 MEDIUM
CVE-2026-61109	6.5 MEDIUM
CVE-2026-61128	4.9 MEDIUM
CVE-2026-61144	4.9 MEDIUM

CWE's

CWE	Beschrijving
CWE-404	Improper Resource Shutdown or Release

Getroffen producten

Oracle
Mysql
Mysql Cluster
Mysql Router
Mysql Server

Disclaimer