



NCSC-2026-0315

Kwetsbaarheden verholpen in Oracle MySQL

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 19-08-2026

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 kwetsbaarheden verholpen in Oracle MySQL Cluster en Oracle MySQL Connector/ODBC.

Duiding

Oracle MySQL Cluster versies 8.0.0 tot 8.0.48, 8.4.0 tot 8.4.11 en 9.7.0 tot 9.7.2 bevatten kwetsbaarheden die een niet-geauthenticeerde externe aanvaller via netwerktoegang toestaan denial of service te veroorzaken, ongeautoriseerde datamodificatie uit te voeren of het systeem over te nemen, waarbij sommig misbruik gebruikersinteractie vereisen.

Oracle MySQL Connector/ODBC versie 26.7.0 bevat meerdere kwetsbaarheden die een niet-geauthenticeerde aanvaller met infrastructuurtoegang en soms gebruikersinteractie toestaan denial of service te veroorzaken door crashes, en in sommige gevallen ongeautoriseerde leestoegang tot data verkrijgen, wat de beschikbaarheid en vertrouwelijkheid beïnvloedt.

Oplossingen

Oracle heeft updates uitgebracht om de kwetsbaarheden in Oracle MySQL Cluster en Oracle MySQL Connector/ODBC te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://www.oracle.com/security-alerts/cspuaug2026.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-13151	7.5 HIGH
➤ CVE-2025-14821	7.8 HIGH
➤ CVE-2026-0968	3.1 LOW
➤ CVE-2026-60592	8.2 HIGH
➤ CVE-2026-65914	6.9 MEDIUM
➤ CVE-2026-70724	7.5 HIGH

> CVE-2026-71073	5.5 MEDIUM
> CVE-2026-71079	6.5 MEDIUM
> CVE-2026-71084	6.8 MEDIUM

CWE's

CWE	Beschrijving
> CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
> CWE-426	Untrusted Search Path
> CWE-427	Uncontrolled Search Path Element
> CWE-476	NULL Pointer Dereference
> CWE-787	Out-of-bounds Write

Getroffen producten

Oracle
MySQL
MySQL Cluster
MySQL Connectors

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.