



Advisory NCSC-2026-0441

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Oracle MySQL

Publicatiedatum: 21-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Oracle heeft kwetsbaarheden verholpen in diverse producten, waaronder Oracle MySQL Server, MySQL Cluster, MySQL Enterprise Backup, MySQL Connectors (waaronder Connector/ODBC) en MySQL Router.

Duiding

De kwetsbaarheden in Oracle MySQL betreffen diverse componenten, waaronder MySQL Server, MySQL Cluster, MySQL Enterprise Backup, MySQL Connectors en MySQL Router. De potentiële impact omvat ongeautoriseerde toegang tot of wijziging van gegevens en verstoring van de beschikbaarheid van systemen (denial-of-service). De Oracle Critical Patch Update van oktober 2026 bevat 98 nieuwe beveiligingspatches, waarvan 29 kwetsbaarheden op afstand kunnen worden misbruikt zonder authenticatie. De hoogste CVSS-score bedraagt 9,8. De ernst en impact verschillen per kwetsbaarheid en zijn afhankelijk van de getroffen component en configuratie.

Oplossingen

OpenSSL, curl en Oracle hebben updates uitgebracht om de kwetsbaarheden in hun respectievelijke producten te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://www.oracle.com/security-alerts/cpuoct2026.html>

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-15467	9.8 CRITICAL
CVE-2026-9547	9.8 CRITICAL
CVE-2026-83404	7.5 HIGH
CVE-2026-101679	7.5 HIGH
CVE-2026-101768	8.1 HIGH

CVE	CVSS Score
CVE-2026-101769	7.0 HIGH
CVE-2026-101770	8.1 HIGH
CVE-2026-101771	8.1 HIGH
CVE-2026-101772	8.1 HIGH
CVE-2026-101773	7.1 HIGH
CVE-2026-101775	7.4 HIGH
CVE-2026-101781	8.8 HIGH
CVE-2026-101783	7.4 HIGH
CVE-2026-101785	8.3 HIGH
CVE-2026-101786	7.2 HIGH
CVE-2026-101796	7.5 HIGH
CVE-2026-101797	7.5 HIGH
CVE-2026-101810	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-297	Improper Validation of Certificate with Host Mismatch
CWE-347	Improper Verification of Cryptographic Signature
CWE-787	Out-of-bounds Write

Getroffen producten

Oracle
MySQL
MySQL Cluster
MySQL Connectors
MySQL Enterprise Backup
MySQL Server

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 or 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.