



CVE-2017-3599

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2017-3599
State	PUBLIC
Assigner	secalert_us@oracle.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-24 19:59:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Pluggable Auth). Supported versio

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Mysql	All	All	All	All
Application	Oracle	Mysql	All	All	All	All

References

Reference

- MySQL Multiple Flaws Let Remote Authenticated and Local Users Modify Data, Remote and Local Users Deny Service, and Remote Authent...
- Oracle Critical Patch Update - April 2017
- Red Hat Customer Portal
- Pre-Auth MySQL remote DOS (Integer Overflow) | SECFORCE
- Oracle MySQL Server CVE-2017-3599 Remote Security Vulnerability
- Exploit – Page 41954 – Exploits Database
- Red Hat Customer Portal
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

710243 Gentoo Linux MySQL Multiple Vulnerabilities (GLSA 201802-04)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)