



# CVE-2013-3794

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

## Summary

|                        |                                                                                                                        |
|------------------------|------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2013-3794                                                                                                          |
| <b>State</b>           | PUBLIC                                                                                                                 |
| <b>Assigner</b>        | secalert_us@oracle.com                                                                                                 |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                           |
| <b>Published</b>       | 2013-07-17 13:41:00 UTC                                                                                                |
| <b>Updated</b>         | 2022-08-29 20:53:00 UTC                                                                                                |
| <b>Description</b>     | Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.30 and earlier and 5.6.10 allows remote au |

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                   | Product                  | Version | Update | Edition | Language |
|------------------|--------------------------|--------------------------|---------|--------|---------|----------|
| Application      | <a href="#">Mariadb</a>  | <a href="#">Mariadb</a>  | All     | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a> | <a href="#">Opensuse</a> | 11.4    | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a> | <a href="#">Opensuse</a> | 12.2    | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a> | <a href="#">Opensuse</a> | 12.3    | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a> | <a href="#">Opensuse</a> | 11.4    | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a> | <a href="#">Opensuse</a> | 12.2    | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a> | <a href="#">Opensuse</a> | 12.3    | All    | All     | All      |
| Application      | <a href="#">Oracle</a>   | <a href="#">Mysql</a>    | 5.5.0   | All    | All     | All      |
| Application      | <a href="#">Oracle</a>   | <a href="#">Mysql</a>    | 5.5.1   | All    | All     | All      |
| Application      | <a href="#">Oracle</a>   | <a href="#">Mysql</a>    | 5.5.10  | All    | All     | All      |
| Application      | <a href="#">Oracle</a>   | <a href="#">Mysql</a>    | 5.5.11  | All    | All     | All      |
| Application      | <a href="#">Oracle</a>   | <a href="#">Mysql</a>    | 5.5.12  | All    | All     | All      |
| Application      | <a href="#">Oracle</a>   | <a href="#">Mysql</a>    | 5.5.13  | All    | All     | All      |
| Application      | <a href="#">Oracle</a>   | <a href="#">Mysql</a>    | 5.5.14  | All    | All     | All      |
| Application      | <a href="#">Oracle</a>   | <a href="#">Mysql</a>    | 5.5.15  | All    | All     | All      |
| Application      | <a href="#">Oracle</a>   | <a href="#">Mysql</a>    | 5.5.16  | All    | All     | All      |
| Application      | <a href="#">Oracle</a>   | <a href="#">Mysql</a>    | 5.5.17  | All    | All     | All      |

|             |        |       |        |     |     |     |
|-------------|--------|-------|--------|-----|-----|-----|
|             |        |       |        |     |     |     |
| Application | Oracle | Mysql | 5.5.18 | All | All | All |
| Application | Oracle | Mysql | 5.5.19 | All | All | All |
| Application | Oracle | Mysql | 5.5.2  | All | All | All |
| Application | Oracle | Mysql | 5.5.20 | All | All | All |
| Application | Oracle | Mysql | 5.5.21 | All | All | All |
| Application | Oracle | Mysql | 5.5.22 | All | All | All |
| Application | Oracle | Mysql | 5.5.23 | All | All | All |
| Application | Oracle | Mysql | 5.5.24 | All | All | All |
| Application | Oracle | Mysql | 5.5.25 | All | All | All |
| Application | Oracle | Mysql | 5.5.25 | a   | All | All |
| Application | Oracle | Mysql | 5.5.26 | All | All | All |
| Application | Oracle | Mysql | 5.5.27 | All | All | All |
| Application | Oracle | Mysql | 5.5.28 | All | All | All |
| Application | Oracle | Mysql | 5.5.29 | All | All | All |
| Application | Oracle | Mysql | 5.5.3  | All | All | All |
| Application | Oracle | Mysql | 5.5.4  | All | All | All |
| Application | Oracle | Mysql | 5.5.5  | All | All | All |
| Application | Oracle | Mysql | 5.5.6  | All | All | All |
| Application | Oracle | Mysql | 5.5.7  | All | All | All |
| Application | Oracle | Mysql | 5.5.9  | All | All | All |
| Application | Oracle | Mysql | 5.6.0  | All | All | All |
| Application | Oracle | Mysql | 5.6.1  | All | All | All |
| Application | Oracle | Mysql | 5.6.2  | All | All | All |
| Application | Oracle | Mysql | 5.6.3  | All | All | All |
| Application | Oracle | Mysql | 5.6.4  | All | All | All |
| Application | Oracle | Mysql | 5.6.5  | All | All | All |
| Application | Oracle | Mysql | 5.6.6  | All | All | All |
| Application | Oracle | Mysql | 5.6.7  | All | All | All |
| Application | Oracle | Mysql | 5.6.8  | All | All | All |
| Application | Oracle | Mysql | 5.6.9  | All | All | All |
| Application | Oracle | Mysql | 5.5.0  | All | All | All |
| Application | Oracle | Mysql | 5.5.1  | All | All | All |
| Application | Oracle | Mysql | 5.5.10 | All | All | All |
| Application | Oracle | Mysql | 5.5.11 | All | All | All |
| Application | Oracle | Mysql | 5.5.12 | All | All | All |

|             |        |       |        |     |     |     |
|-------------|--------|-------|--------|-----|-----|-----|
| Application | Oracle | Mysql | 5.5.13 | All | All | All |
| Application | Oracle | Mysql | 5.5.14 | All | All | All |
| Application | Oracle | Mysql | 5.5.15 | All | All | All |
| Application | Oracle | Mysql | 5.5.16 | All | All | All |
| Application | Oracle | Mysql | 5.5.17 | All | All | All |
| Application | Oracle | Mysql | 5.5.18 | All | All | All |
| Application | Oracle | Mysql | 5.5.19 | All | All | All |
| Application | Oracle | Mysql | 5.5.2  | All | All | All |
| Application | Oracle | Mysql | 5.5.20 | All | All | All |
| Application | Oracle | Mysql | 5.5.21 | All | All | All |
| Application | Oracle | Mysql | 5.5.22 | All | All | All |
| Application | Oracle | Mysql | 5.5.23 | All | All | All |
| Application | Oracle | Mysql | 5.5.24 | All | All | All |
| Application | Oracle | Mysql | 5.5.25 | All | All | All |
| Application | Oracle | Mysql | 5.5.25 | a   | All | All |
| Application | Oracle | Mysql | 5.5.26 | All | All | All |
| Application | Oracle | Mysql | 5.5.27 | All | All | All |
| Application | Oracle | Mysql | 5.5.28 | All | All | All |
| Application | Oracle | Mysql | 5.5.29 | All | All | All |
| Application | Oracle | Mysql | 5.5.3  | All | All | All |
| Application | Oracle | Mysql | 5.5.4  | All | All | All |
| Application | Oracle | Mysql | 5.5.5  | All | All | All |
| Application | Oracle | Mysql | 5.5.6  | All | All | All |
| Application | Oracle | Mysql | 5.5.7  | All | All | All |
| Application | Oracle | Mysql | 5.5.9  | All | All | All |
| Application | Oracle | Mysql | 5.6.0  | All | All | All |
| Application | Oracle | Mysql | 5.6.1  | All | All | All |
| Application | Oracle | Mysql | 5.6.2  | All | All | All |
| Application | Oracle | Mysql | 5.6.3  | All | All | All |
| Application | Oracle | Mysql | 5.6.4  | All | All | All |
| Application | Oracle | Mysql | 5.6.5  | All | All | All |
| Application | Oracle | Mysql | 5.6.6  | All | All | All |
| Application | Oracle | Mysql | 5.6.7  | All | All | All |
| Application | Oracle | Mysql | 5.6.8  | All | All | All |
| Application | Oracle | Mysql | 5.6.9  | All | All | All |
| Application | Oracle | Mysql | 5.6.9  | All | All | All |

|                  |        |                                                |      |     |     |     |
|------------------|--------|------------------------------------------------|------|-----|-----|-----|
| Application      | Oracle | Mysql                                          | All  | All | All | All |
| Application      | Oracle | Mysql                                          | All  | All | All | All |
| Operating System | Oracle | Solaris                                        | 11.3 | All | All | All |
| Operating System | Oracle | Solaris                                        | 11.3 | All | All | All |
| Operating System | Suse   | Linux Enterprise Desktop                       | 11   | sp3 | All | All |
| Operating System | Suse   | Linux Enterprise Server                        | 11   | sp3 | All | All |
| Operating System | Suse   | Linux Enterprise Server                        | 11   | sp3 | All | All |
| Operating System | Suse   | Linux Enterprise Software Development Kit      | 11   | sp3 | All | All |
| Operating System | Suse   | Suse Linux Enterprise Desktop                  | 11.0 | sp3 | All | All |
| Operating System | Suse   | Suse Linux Enterprise Desktop                  | 11.0 | sp3 | All | All |
| Operating System | Suse   | Suse Linux Enterprise Server                   | 11.0 | sp3 | All | All |
| Operating System | Suse   | Suse Linux Enterprise Server                   | 11.0 | sp3 | All | All |
| Operating System | Suse   | Suse Linux Enterprise Server                   | 11.0 | sp3 | All | All |
| Operating System | Suse   | Suse Linux Enterprise Server                   | 11.0 | sp3 | All | All |
| Application      | Suse   | Suse Linux Enterprise Software Development Kit | 11.0 | sp3 | All | All |
| Application      | Suse   | Suse Linux Enterprise Software Development Kit | 11.0 | sp3 | All | All |

| References                                                               |         |                                                                   |                      |
|--------------------------------------------------------------------------|---------|-------------------------------------------------------------------|----------------------|
| Reference                                                                | Source  | Link                                                              | Tags                 |
| [security-announce] SUSE-SU-2013:1390-1: important: Security update for  | SUSE    | <a href="https://lists.opensuse.org">lists.opensuse.org</a>       | Third Party Advisory |
| Oracle Critical Patch Update - July 2013                                 | CONFIRM | <a href="https://www.oracle.com">www.oracle.com</a>               | Vendor Advisory      |
| openSUSE-SU-2013:1410-1: moderate: update for mysql-community-server     | SUSE    | <a href="https://lists.opensuse.org">lists.opensuse.org</a>       | Third Party Advisory |
| Oracle Solaris Third Party Bulletin - October 2015                       | CONFIRM | <a href="https://www.oracle.com">www.oracle.com</a>               | Vendor Advisory      |
| Oracle MySQL Server CVE-2013-3794 Remote Security Vulnerability          | BID     | <a href="https://www.securityfocus.com">www.securityfocus.com</a> | Third Party Advisory |
| openSUSE-SU-2013:1335-1: moderate: update for mariadb, mysql-community-s | SUSE    | <a href="https://lists.opensuse.org">lists.opensuse.org</a>       | Third Party Advisory |
| [security-announce] SUSE-SU-2013:1529-1: important: Security update for  | SUSE    | <a href="https://lists.opensuse.org">lists.opensuse.org</a>       | Third Party Advisory |
| 95333                                                                    | OSVDB   | <a href="https://osvdb.org">osvdb.org</a>                         | Broken Link          |
| CVE Program record                                                       | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>                     | canonical            |
| NVD vulnerability detail                                                 | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                   | canonical, analysis  |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)