



CVE-2014-2494

Published on: 07/16/2014 12:00:00 AM UTC

Last Modified on: 08/26/2022 04:12:00 PM UTC

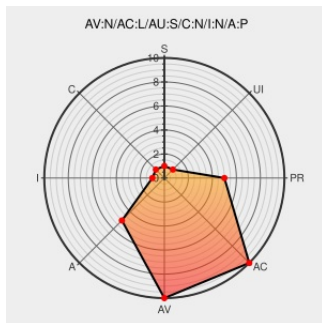
CVE-2014-2494

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.37 and earlier allows remote authenticated users to affect availability via vectors related to ENARC.

CVE-2014-2494 has been assigned by secalert_us@oracle.com to track the vulnerability

CVSS2 Score: **4 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

SINGLE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

NONE

PARTIAL

CVE References

Description

Tags

Link

MySQL Multiple Bugs Let Remote Authenticated Users Partially Access and Modify Data and Partially Deny Service - SecurityTracker

www.securitytracker.com
text/html

[SECTrack 1030578](#)

[security-announce] SUSE-SU-2014:1072-1: important: Security update for

lists.opensuse.org
text/html

[SUSE SUSE-SU-2014:1072](#)

VMSA-2014-0012 | United States

www.vmware.com
text/html

[CONFIRM www.vmware.com/security/advisories/VMSA-2014-0012.html](#)

Debian -- Security Information -- DSA-2985-1 mysql-5.5

www.debian.org
Deprecated Link
text/html

[DEBIAN DSA-2985](#)

Oracle Solaris Third Party Bulletin - October 2015

www.oracle.com
text/html

[CONFIRM www.oracle.com/technetwork/topics/security/bulletinoct2015-2511968.html](#)

Full Disclosure: NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities	seclists.org text/html	 FULLDISC 20141205 NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities
[security-announce] SUSE-SU-2015:0743-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2015:0743
About Secunia Research Flexera	web.archive.org text/html	 SECUNIA 60425
Oracle Critical Patch Update - July 2014	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	 CONFIRM www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20141205 NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Mariadb	Mariadb	All	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	5.5.20	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	5.5.30	All	All	All
Application	Oracle	Mysql	5.5.31	All	All	All
Application	Oracle	Mysql	5.5.32	All	All	All
Application	Oracle	Mysql	5.5.33	All	All	All
Application	Oracle	Mysql	5.5.34	All	All	All
Application	Oracle	Mysql	5.5.35	All	All	All
Application	Oracle	Mysql	5.5.36	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	5.5.20	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	5.5.30	All	All	All
Application	Oracle	Mysql	5.5.31	All	All	All

Application	Oracle	Mysql	5.5.32	All	All	All
Application	Oracle	Mysql	5.5.33	All	All	All
Application	Oracle	Mysql	5.5.34	All	All	All
Application	Oracle	Mysql	5.5.35	All	All	All
Application	Oracle	Mysql	5.5.36	All	All	All
Application	Oracle	Mysql	All	All	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	12	-	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 Server	12	-	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	-	All	All
Operating System	Suse	Linux Enterprise Workstation Extension	12	-	All	All
cpe:2.3:o:debian:debian_linux:7.0:****:*:*:*:						
cpe:2.3:a:mariadb:mariadb:****:*:*:*:						
cpe:2.3:a:oracle:mysql:5.5.10:*****:*:*:						
cpe:2.3:a:oracle:mysql:5.5.11:*****:*:*:						
cpe:2.3:a:oracle:mysql:5.5.12:*****:*:*:						
cpe:2.3:a:oracle:mysql:5.5.13:*****:*:*:						
cpe:2.3:a:oracle:mysql:5.5.14:*****:*:*:						
cpe:2.3:a:oracle:mysql:5.5.15:*****:*:*:						
cpe:2.3:a:oracle:mysql:5.5.16:*****:*:*:						
cpe:2.3:a:oracle:mysql:5.5.17:*****:*:*:						
cpe:2.3:a:oracle:mysql:5.5.18:*****:*:*:						
cpe:2.3:a:oracle:mysql:5.5.19:*****:*:*:						
cpe:2.3:a:oracle:mysql:5.5.20:*****:*:*:						

```
cpe:2.3:a:oracle:mysql:5.5.21:::*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.22:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.23:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:oracle:mysql:5.5.24:*:*:*:*:*:
```

cpe:2.3:a:oracle:mysql:5.5.25:*:*:*:*:*:*:

```
cpe:2.3:a:oracle:mysql:5.5.25:a:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.26:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.27:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.28:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.29:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.30:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.31:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:oracle:mysql:5.5.32:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.33:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.34:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.35:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.36:.*:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:oracle:mysql:5.5.10:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.11:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.12:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.13:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.14:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.15:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.16:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.17:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.18:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.19:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.20:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.21:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.22:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.23:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.24:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.25:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.25:a:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.26:*:*:*:*:*:*:
```

cpe:2.3:a:oracle:mysql:5.5.27:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.5.28:*:*:*:*:*:*:

```
cpe:2.3:a:oracle:mysql:5.5.29:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.30:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.31:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.32:*:*:*:*:*:*:
```

cpe:2.3:a:oracle:mysql:5.5.33:*:*:*:*:*:*:

```
cpe:2.3:a:oracle:mysql:5.5.34:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.35:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:5.5.36:*:*:*:*:*:*:
```

```
cpe:2.3:a:oracle:mysql:*.:*:*:*:*:*:*:
```

```
cpe:2.3:o:suse:linux_enterprise_desktop:11:sp3:*:*:*:*:*
```

```
cpe:2.3:o:suse:linux_enterprise_desktop:12:-:*:*:*:*:*:
```

```
cpe:2.3:o:suse:linux_enterprise_server:11:sp3:*:*:*:-:*:*
```

```
cpe:2.3:o:suse:linux_enterprise_server:11:sp3:*:*:*:vmware:*:*:
```

```
cpe:2.3:o:suse:linux_enterprise_server:12:-:*:*:*:*:*:
```

```
cpe:2.3:o:suse:linux_enterprise_software_development_kit:11:sp3:*:*:*.*.*
```

```
cpe:2.3:o:suse:linux_enterprise_software_development_kit:12:-:*:*:*:*.*
```

```
cpe:2.3:o:suse:linux_enterprise_workstation_extension:12:-:*:*:*:*:
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© [CVE.report](#) 2023   |

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](#)