



# CVE-2013-7252

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

## Summary

|                        |                                                                                                                     |
|------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2013-7252                                                                                                       |
| <b>State</b>           | PUBLIC                                                                                                              |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                 |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                        |
| <b>Published</b>       | 2015-01-18 18:59:00 UTC                                                                                             |
| <b>Updated</b>         | 2016-08-02 13:58:00 UTC                                                                                             |
| <b>Description</b>     | kwalletd in KWallet before KDE Applications 14.12.0 uses Blowfish with ECB mode instead of CBC mode when encrypting |

## Risk And Classification

### Problem Types: CWE-310

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor              | Product                          | Version | Update | Edition | Language |
|-------------|---------------------|----------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Kde</a> | <a href="#">Kde Applications</a> | All     | All    | All     | All      |

## References

| Reference                                                                  | Source  | Link                                  | Tags                   |
|----------------------------------------------------------------------------|---------|---------------------------------------|------------------------|
| Bug 1048168 – CVE-2013-7252 kwallet: crypto misuse                         | CONFIRM | <a href="#">bugzilla.redhat.com</a>   | Issue Tracking         |
| oss-security - Re: CVE Request: kwallet: incorrect CBC encryption handling | MLIST   | <a href="#">www.openwall.com</a>      |                        |
| oss-security - kwallet crypto misuse                                       | MLIST   | <a href="#">www.openwall.com</a>      |                        |
| <a href="#">www.kde.org/info/security/advisory-20150109-1.txt</a>          | CONFIRM | <a href="#">www.kde.org</a>           | Patch, Vendor Advisory |
| kwallet Weak Stored Password Encryption Local Security Weakness            | BID     | <a href="#">www.securityfocus.com</a> | Third Party Advisory   |
| kwalletd: Information disclosure (GLSA 201606-19) — Gentoo security        | GENTOO  | <a href="#">security.gentoo.org</a>   | Third Party Advisory   |
| KWallet Security Analysis   Gaganpreet's blog                              | MISC    | <a href="#">gaganpreet.in</a>         | Exploit                |
| CVE Program record                                                         | CVE.ORG | <a href="#">www.cve.org</a>           | canonical              |
| NVD vulnerability detail                                                   | NVD     | <a href="#">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.

© [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](#).

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

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