



# CVE-2012-5621

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

## Summary

|                        |                                                                                                                                                       |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2012-5621                                                                                                                                         |
| <b>State</b>           | PUBLIC                                                                                                                                                |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                                                   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                                          |
| <b>Published</b>       | 2014-09-29 22:55:00 UTC                                                                                                                               |
| <b>Updated</b>         | 2017-08-29 01:32:00 UTC                                                                                                                               |
| <b>Description</b>     | lib/engine/components/opal/opal-call.cpp in ekiga before 4.0.0 allows remote attackers to cause a denial of service (crash) via crafted SIP messages. |

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

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

## References

| Reference                                                                                                                  | Source  | Link                                         |
|----------------------------------------------------------------------------------------------------------------------------|---------|----------------------------------------------|
| Validate UTF-8 strings before showing them (7d098072) · Commits · GNOME / ekiga · GitLab                                   | CONFIRM | <a href="#">gitlab.com</a>                   |
| CVE-2012-5621 Denial of Service (DoS) vulnerability in Ekiga (Third Party Vulnerability Resolution Blog)                   | CONFIRM | <a href="#">blog.ekiga.org</a>               |
| ftp.gnome.org/pub/gnome/sources/ekiga/4.0/ekiga-4.0.0.news                                                                 | CONFIRM | <a href="#">ftp.gnome.org</a>                |
| [SECURITY] Fedora 18 Update: opal-3.10.10-1.fc18                                                                           | FEDORA  | <a href="#">lists.fedoraproject.org</a>      |
| oss-sec: Re: CVE Request -- Ekiga (x < 4.0.0): DoS (crash) after receiving call from other party with not UTF-8 valid name | MLIST   | <a href="#">secalert@redhat.com</a>          |
| Ekiga UTF-8 Parsing Denial of Service Vulnerability                                                                        | BID     | <a href="#">www.bidsa.org</a>                |
| IBM X-Force Exchange                                                                                                       | XF      | <a href="#">exchange.xforce.ibmcloud.com</a> |
| Bug 883058 – CVE-2012-5621 ekiga: DoS (crash) after receiving call from other party with not UTF-8 valid name              | CONFIRM | <a href="#">bugzilla.gnome.org</a>           |
| CVE Program record                                                                                                         | CVE.ORG | <a href="#">www.cve.org</a>                  |
| NVD vulnerability detail                                                                                                   | NVD     | <a href="#">nvd.nist.gov</a>                 |

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](#)