



# CVE-2014-8106

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

## Summary

|                        |                                                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2014-8106                                                                                                             |
| <b>State</b>           | PUBLIC                                                                                                                    |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                       |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                              |
| <b>Published</b>       | 2014-12-08 16:59:00 UTC                                                                                                   |
| <b>Updated</b>         | 2023-02-13 00:42:00 UTC                                                                                                   |
| <b>Description</b>     | Heap-based buffer overflow in the Cirrus VGA emulator (hw/display/cirrus_vga.c) in QEMU before 2.2.0 allows local guest u |

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor               | Product              | Version | Update | Edition | Language |
|-------------|----------------------|----------------------|---------|--------|---------|----------|
| Application | <a href="#">Qemu</a> | <a href="#">Qemu</a> | 2.1.0   | All    | All     | All      |
| Application | <a href="#">Qemu</a> | <a href="#">Qemu</a> | 2.1.0   | rc0    | All     | All      |
| Application | <a href="#">Qemu</a> | <a href="#">Qemu</a> | 2.1.0   | rc1    | All     | All      |
| Application | <a href="#">Qemu</a> | <a href="#">Qemu</a> | 2.1.0   | rc2    | All     | All      |
| Application | <a href="#">Qemu</a> | <a href="#">Qemu</a> | 2.1.0   | rc3    | All     | All      |
| Application | <a href="#">Qemu</a> | <a href="#">Qemu</a> | 2.1.0   | rc5    | All     | All      |
| Application | <a href="#">Qemu</a> | <a href="#">Qemu</a> | 2.1.1   | All    | All     | All      |
| Application | <a href="#">Qemu</a> | <a href="#">Qemu</a> | 2.1.0   | All    | All     | All      |
| Application | <a href="#">Qemu</a> | <a href="#">Qemu</a> | 2.1.0   | rc0    | All     | All      |
| Application | <a href="#">Qemu</a> | <a href="#">Qemu</a> | 2.1.0   | rc1    | All     | All      |
| Application | <a href="#">Qemu</a> | <a href="#">Qemu</a> | 2.1.0   | rc2    | All     | All      |
| Application | <a href="#">Qemu</a> | <a href="#">Qemu</a> | 2.1.0   | rc3    | All     | All      |
| Application | <a href="#">Qemu</a> | <a href="#">Qemu</a> | 2.1.0   | rc5    | All     | All      |
| Application | <a href="#">Qemu</a> | <a href="#">Qemu</a> | 2.1.1   | All    | All     | All      |
| Application | <a href="#">Qemu</a> | <a href="#">Qemu</a> | All     | All    | All     | All      |

## References

| Reference                                                                                         | Source  | Link                                                                           |
|---------------------------------------------------------------------------------------------------|---------|--------------------------------------------------------------------------------|
| Citrix XenServer Multiple Security Updates                                                        | CONFIRM | <a href="http://support.citrix.com">support.citrix.com</a>                     |
| <a href="http://access.redhat.com">access.redhat.com</a>   CVE-2014-8106                          | MISC    | <a href="http://access.redhat.com">access.redhat.com</a>                       |
| Red Hat Customer Portal                                                                           | MISC    | <a href="http://access.redhat.com">access.redhat.com</a>                       |
| Red Hat Customer Portal                                                                           | REDHAT  | <a href="http://rhn.redhat.com">rhn.redhat.com</a>                             |
| Red Hat Customer Portal                                                                           | MISC    | <a href="http://access.redhat.com">access.redhat.com</a>                       |
| Debian -- Security Information -- DSA-3087-1 qemu                                                 | DEBIAN  | <a href="http://www.debian.org">www.debian.org</a>                             |
| Security Advisory SA60364 - QEMU Cirrus VGA Driver Blit Region Handling Vulnerabilities - Secunia | SECUNIA | <a href="http://secunia.com">secunia.com</a>                                   |
| <a href="http://git.qemu.org">git.qemu.org</a> Git - qemu.git/commit                              | MISC    | <a href="http://git.qemu.org">git.qemu.org</a>                                 |
| Red Hat Customer Portal - Access to 24x7 support and knowledge                                    | MISC    | <a href="http://access.redhat.com">access.redhat.com</a>                       |
| Red Hat Customer Portal                                                                           | REDHAT  | <a href="http://rhn.redhat.com">rhn.redhat.com</a>                             |
| [SECURITY] Fedora 21 Update: qemu-2.1.3-5.fc21                                                    | FEDORA  | <a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a>           |
| [Qemu-devel] [PULL for-2.2 0/2] cirrus: fix blit region check (cve-2014-                          | MLIST   | <a href="http://lists.gnu.org">lists.gnu.org</a>                               |
| Debian -- Security Information -- DSA-3088-1 qemu-kvm                                             | DEBIAN  | <a href="http://www.debian.org">www.debian.org</a>                             |
| Red Hat Customer Portal                                                                           | REDHAT  | <a href="http://rhn.redhat.com">rhn.redhat.com</a>                             |
| <a href="http://git.qemu.org">git.qemu.org</a> Git                                                | MISC    | <a href="http://git.qemu.org">git.qemu.org</a>                                 |
| Red Hat Customer Portal                                                                           | REDHAT  | <a href="http://rhn.redhat.com">rhn.redhat.com</a>                             |
| Red Hat Customer Portal                                                                           | REDHAT  | <a href="http://rhn.redhat.com">rhn.redhat.com</a>                             |
| Red Hat Customer Portal                                                                           | MISC    | <a href="http://access.redhat.com">access.redhat.com</a>                       |
| IBM X-Force Exchange                                                                              | XF      | <a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a> |
| 1169454 – (CVE-2014-8106) CVE-2014-8106 qemu: cirrus: insufficient blit region checks             | MISC    | <a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>                   |
| oss-security - CVE-2014-8106 qemu: cirrus: insufficient blit region checks                        | MLIST   | <a href="http://www.openwall.com">www.openwall.com</a>                         |
| QEMU 'cirrus_vga.c' Security Bypass Vulnerability                                                 | BID     | <a href="http://www.securityfocus.com">www.securityfocus.com</a>               |
| Red Hat Customer Portal                                                                           | MISC    | <a href="http://access.redhat.com">access.redhat.com</a>                       |
| Red Hat Customer Portal                                                                           | MISC    | <a href="http://access.redhat.com">access.redhat.com</a>                       |
| <a href="http://git.qemu.org">git.qemu.org</a> Git - qemu.git/commit                              | CONFIRM | <a href="http://git.qemu.org">git.qemu.org</a>                                 |
| Red Hat Customer Portal                                                                           | REDHAT  | <a href="http://rhn.redhat.com">rhn.redhat.com</a>                             |
| <a href="http://git.qemu.org">git.qemu.org</a> Git - qemu.git/commit                              | CONFIRM | <a href="http://git.qemu.org">git.qemu.org</a>                                 |
| Red Hat Customer Portal                                                                           | REDHAT  | <a href="http://rhn.redhat.com">rhn.redhat.com</a>                             |
| Red Hat Customer Portal                                                                           | MISC    | <a href="http://access.redhat.com">access.redhat.com</a>                       |
| CVE Program record                                                                                | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                                   |
| NVD vulnerability detail                                                                          | NVD     | <a href="http://nvd.nist.gov">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](#)