



# CVE-2012-4411

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

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2012-4411                                                                                                               |
| <b>State</b>           | PUBLIC                                                                                                                      |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                         |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                |
| <b>Published</b>       | 2012-11-23 20:55:00 UTC                                                                                                     |
| <b>Updated</b>         | 2023-11-07 02:11:00 UTC                                                                                                     |
| <b>Description</b>     | The graphical console in Xen 4.0, 4.1 and 4.2 allows local OS guest administrators to obtain sensitive host resource inform |

## Risk And Classification

### Problem Types: CWE-200

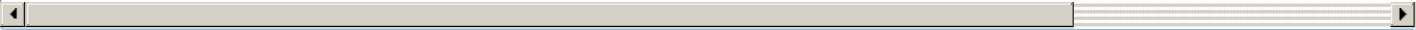
## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor              | Product             | Version | Update | Edition | Language |
|------------------|---------------------|---------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 4.0.0   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 4.1.0   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 4.2.0   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 4.0.0   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 4.1.0   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 4.2.0   | All    | All     | All      |

## References

| Reference                                                                                         | Source  | Link                        |
|---------------------------------------------------------------------------------------------------|---------|-----------------------------|
| Security Advisory SA50493 - Xen Qemu Monitor Console Privilege Escalation Vulnerability - Secunia | SECUNIA | <a href="#">secunia.c</a>   |
| Debian -- Security Information -- DSA-2543-1 xen-qemu-dm-4.0                                      | DEBIAN  | <a href="#">www.deb</a>     |
| Xen CVE-2012-4411 Local Security Bypass Vulnerability                                             | BID     | <a href="#">www.sec</a>     |
| [security-announce] SUSE-SU-2012:1487-1: important: Security update for                           | SUSE    | <a href="#">lists.oper</a>  |
| Security Advisory SA51352 - SUSE update for libvirt - Secunia                                     | SECUNIA | <a href="#">secunia.c</a>   |
| [security-announce] openSUSE-SU-2012:1572-1: important: XEN: security an                          | SUSE    | <a href="#">lists.oper</a>  |
| [Xen-announce] Xen Security Advisory 19 - guest administrator can access qemu monitor console     | MLIST   | <a href="#">lists.xen.c</a> |
| oss-security - Xen Security Advisory 19 - guest administrator can access qemu monitor console     | MLIST   | <a href="#">www.ope</a>     |

|                                                                                                               |         |                             |
|---------------------------------------------------------------------------------------------------------------|---------|-----------------------------|
| Security Advisory SA51413 - SUSE update for xen - Secunia                                                     | SECUNIA | <a href="#">secunia.c</a>   |
| [Xen-announce] Xen Security Advisory 19 (CVE-2012-4411) - guest administrator can access qemu monitor console | MLIST   | <a href="#">lists.xen.o</a> |
| Security Advisory SA51324 - SUSE update for xen - Secunia                                                     | SECUNIA | <a href="#">secunia.c</a>   |
| oss-security - Xen Security Advisory 19 (CVE-2012-4411) - guest administrator can access qemu monitor console | MLIST   | <a href="#">www.ope</a>     |
| Security Advisory SA55082 - Gentoo update for xen - Secunia                                                   | SECUNIA | <a href="#">secunia.c</a>   |
| oss-security - Re: Xen Security Advisory 19 - guest administrator can access qemu monitor console             | MLIST   | <a href="#">www.ope</a>     |
| Gentoo Linux Documentation -- Xen: Multiple vulnerabilities                                                   | GENTOO  | <a href="#">security.g</a>  |
| [security-announce] openSUSE-SU-2012:1573-1: important: XEN: security an                                      | SUSE    | <a href="#">lists.oper</a>  |
| [security-announce] SUSE-SU-2012:1486-1: important: Security update for                                       | SUSE    | <a href="#">lists.oper</a>  |
| Xen: Multiple vulnerabilities (GLSA 201604-03) — Gentoo Security                                              | GENTOO  | <a href="#">security.g</a>  |
| [security-announce] SUSE-SU-2014:0446-1: important: Security update for                                       | SUSE    | <a href="#">lists.oper</a>  |
| CVE Program record                                                                                            | CVE.ORG | <a href="#">www.cve</a>     |
| NVD vulnerability detail                                                                                      | NVD     | <a href="#">nvd.nist.g</a>  |



No vendor comments have been submitted for this CVE.

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