



# CVE-2012-5514

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

## Summary

|                        |                                                                                                                    |
|------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2012-5514                                                                                                      |
| <b>State</b>           | PUBLIC                                                                                                             |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                       |
| <b>Published</b>       | 2012-12-13 11:53:00 UTC                                                                                            |
| <b>Updated</b>         | 2017-08-29 01:32:00 UTC                                                                                            |
| <b>Description</b>     | The guest_physmap_mark_populate_on_demand function in Xen 4.2 and earlier does not properly unlock the subject GFN |

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor              | Product             | Version | Update | Edition | Language |
|------------------|---------------------|---------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 3.0.2   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 3.0.3   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 3.0.4   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 3.1.3   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 3.1.4   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 3.2.0   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 3.2.1   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 3.2.2   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 3.2.3   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 3.3.0   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 3.3.1   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 3.3.2   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 3.4.0   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 3.4.1   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 3.4.2   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 3.4.3   | All    | All     | All      |
| Operating System | <a href="#">Xen</a> | <a href="#">Xen</a> | 3.4.4   | All    | All     | All      |

|                  |     |     |       |     |     |     |
|------------------|-----|-----|-------|-----|-----|-----|
|                  |     |     |       |     |     |     |
| Operating System | Xen | Xen | 4.0.0 | All | All | All |
| Operating System | Xen | Xen | 4.0.1 | All | All | All |
| Operating System | Xen | Xen | 4.0.2 | All | All | All |
| Operating System | Xen | Xen | 4.0.3 | All | All | All |
| Operating System | Xen | Xen | 4.0.4 | All | All | All |
| Operating System | Xen | Xen | 4.1.0 | All | All | All |
| Operating System | Xen | Xen | 4.1.1 | All | All | All |
| Operating System | Xen | Xen | 4.1.2 | All | All | All |
| Operating System | Xen | Xen | 4.1.3 | All | All | All |
| Operating System | Xen | Xen | 3.0.2 | All | All | All |
| Operating System | Xen | Xen | 3.0.3 | All | All | All |
| Operating System | Xen | Xen | 3.0.4 | All | All | All |
| Operating System | Xen | Xen | 3.1.3 | All | All | All |
| Operating System | Xen | Xen | 3.1.4 | All | All | All |
| Operating System | Xen | Xen | 3.2.0 | All | All | All |
| Operating System | Xen | Xen | 3.2.1 | All | All | All |
| Operating System | Xen | Xen | 3.2.2 | All | All | All |
| Operating System | Xen | Xen | 3.2.3 | All | All | All |
| Operating System | Xen | Xen | 3.3.0 | All | All | All |
| Operating System | Xen | Xen | 3.3.1 | All | All | All |
| Operating System | Xen | Xen | 3.3.2 | All | All | All |
| Operating System | Xen | Xen | 3.4.0 | All | All | All |
| Operating System | Xen | Xen | 3.4.1 | All | All | All |
| Operating System | Xen | Xen | 3.4.2 | All | All | All |
| Operating System | Xen | Xen | 3.4.3 | All | All | All |
| Operating System | Xen | Xen | 3.4.4 | All | All | All |
| Operating System | Xen | Xen | 4.0.0 | All | All | All |
| Operating System | Xen | Xen | 4.0.1 | All | All | All |
| Operating System | Xen | Xen | 4.0.2 | All | All | All |
| Operating System | Xen | Xen | 4.0.3 | All | All | All |
| Operating System | Xen | Xen | 4.0.4 | All | All | All |
| Operating System | Xen | Xen | 4.1.0 | All | All | All |
| Operating System | Xen | Xen | 4.1.1 | All | All | All |
| Operating System | Xen | Xen | 4.1.2 | All | All | All |
| Operating System | Xen | Xen | 4.1.3 | All | All | All |

|                                                                                                                            |     |     |     |     |     |           |
|----------------------------------------------------------------------------------------------------------------------------|-----|-----|-----|-----|-----|-----------|
| Operating System                                                                                                           | Xen | Xen | All | All | All | All       |
|                                                                                                                            |     |     |     |     |     |           |
| References                                                                                                                 |     |     |     |     |     |           |
| Reference                                                                                                                  |     |     |     |     |     | Source    |
| About Secunia Research   Flexera                                                                                           |     |     |     |     |     | SECUNIA   |
| openSUSE-SU-2013:0636-1: moderate: xen: security and bugfix update                                                         |     |     |     |     |     | SUSE      |
| [security-announce] SUSE-SU-2012:1615-1: important: Security update for                                                    |     |     |     |     |     | SUSE      |
| Citrix XenServer Multiple Security Updates                                                                                 |     |     |     |     |     | CONFIRMED |
| About Secunia Research   Flexera                                                                                           |     |     |     |     |     | SECUNIA   |
| openSUSE-SU-2013:0637-1: moderate: xen: security and bugfix update                                                         |     |     |     |     |     | SUSE      |
| 88130                                                                                                                      |     |     |     |     |     | OSVDB     |
| [security-announce] openSUSE-SU-2012:1685-1: important: xen to fix vario                                                   |     |     |     |     |     | SUSE      |
| IBM X-Force Exchange                                                                                                       |     |     |     |     |     | XF        |
| Security Advisory SA51468 - Debian update for xen - Secunia                                                                |     |     |     |     |     | SECUNIA   |
| oss-security - Xen Security Advisory 30 (CVE-2012-5514) - Broken error handling in guest_physmap_mark_populate_on_demand() |     |     |     |     |     | MLIST     |
| Security Advisory SA55082 - Gentoo update for xen - Secunia                                                                |     |     |     |     |     | SECUNIA   |
| About Secunia Research   Flexera                                                                                           |     |     |     |     |     | SECUNIA   |
| [security-announce] openSUSE-SU-2013:0133-1: important: xen to fix vario                                                   |     |     |     |     |     | SUSE      |
| [security-announce] openSUSE-SU-2012:1687-1: important: xen to fix vario                                                   |     |     |     |     |     | SUSE      |
| Gentoo Linux Documentation -- Xen: Multiple vulnerabilities                                                                |     |     |     |     |     | GENTOO    |
| [security-announce] SUSE-SU-2014:0446-1: important: Security update for                                                    |     |     |     |     |     | SUSE      |
| Xen CVE-2012-5514 Local Denial of Service Vulnerability                                                                    |     |     |     |     |     | BID       |
| Debian -- Security Information -- DSA-2582-1 xen                                                                           |     |     |     |     |     | DEBIAN    |
| CVE Program record                                                                                                         |     |     |     |     |     | CVE.O     |
| NVD vulnerability detail                                                                                                   |     |     |     |     |     | NVD       |
| <div><div></div><div></div></div>                                                                                          |     |     |     |     |     |           |
| 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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)