



# CVE-2012-6033

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

## Summary

|                        |                                                                                                                       |
|------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2012-6033                                                                                                         |
| <b>State</b>           | PUBLIC                                                                                                                |
| <b>Assigner</b>        | cve@mitre.org                                                                                                         |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                          |
| <b>Published</b>       | 2012-11-23 20:55:00 UTC                                                                                               |
| <b>Updated</b>         | 2017-08-29 01:32:00 UTC                                                                                               |
| <b>Description</b>     | The do_tmem_control function in the Transcendent Memory (TMEM) in Xen 4.0, 4.1, and 4.2 does not properly check privi |

## Risk And Classification

### Problem Types: CWE-264

## 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                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------|
| Security Announcements - Xen                                                                                                          |
| oss-security - Xen Security Advisory 15 (CVE-2012-3497) - multiple TMEM hypercall vulnerabilities                                     |
| IBM X-Force Exchange                                                                                                                  |
| Xen Transcendent Memory (TMEM) Multiple Flaws Lets Local Users on the Guest Operating System Gain Elevated Privileges on the Host - S |
| [Xen-announce] Xen Security Advisory 15 (CVE-2012-3497) - multiple TMEM hypercall vulnerabilities                                     |
| Security Advisory SA55082 - Gentoo update for xen - Secunia                                                                           |
| Gentoo Linux Documentation -- Xen: Multiple vulnerabilities                                                                           |
| Xen: Multiple vulnerabilities (GLSA 201604-03) — Gentoo Security                                                                      |

Xen 'TMEM hypercall' Multiple Security Vulnerabilities

Security Advisory SA50472 - Xen Multiple Denial of Service and Privilege Escalation Vulnerabilities - Secunia

85199

CVE Program record

NVD vulnerability detail

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](#)