



CVE-2012-6030

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

Summary

CVE	CVE-2012-6030
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-11-23 20:55:00 UTC
Updated	2017-08-29 01:32:00 UTC
Description	The do_tmem_op function in the Transcendent Memory (TMEM) in Xen 4.0, 4.1, and 4.2 allow local guest OS users to cause a denial of service (DoS) by triggering a stack overflow in the do_tmem_op function. This vulnerability is caused by a buffer overflow in the do_tmem_op function. The do_tmem_op function is responsible for handling memory operations in the Transcendent Memory (TMEM) in Xen. It takes a pointer to a memory region and a size, and then copies the data from the memory region to the TMEM. The do_tmem_op function does not check the size of the memory region, which allows an attacker to provide a large memory region and cause a stack overflow. This vulnerability is present in Xen 4.0, 4.1, and 4.2.

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Xen	Xen	4.0.0	All	All	All
Operating System	Xen	Xen	4.1.0	All	All	All
Operating System	Xen	Xen	4.2.0	All	All	All
Operating System	Xen	Xen	4.0.0	All	All	All
Operating System	Xen	Xen	4.1.0	All	All	All
Operating System	Xen	Xen	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.