CVE-2012-6035

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2012-6035
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_destroy_pool function in the Transcendent Memory (TMEM) in Xen 4.0, 4.1, and 4.2 does not properly valida

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.