CVE-2017-12136

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-12136
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-24 14:29:00 UTC
Updated	2019-05-06 12:46:00 UTC
Description	Race condition in the grant table code in Xen 4.6.x through 4.9.x allows local guest OS administrators to cause a denial of s

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Citrix	Xenserver	6.0.2	All	All	All
Application	Citrix	Xenserver	6.2.0	All	All	All
Application	Citrix	Xenserver	6.5	All	All	All
Application	Citrix	Xenserver	7.0	All	All	All
Application	Citrix	Xenserver	7.1	All	All	All
Application	Citrix	Xenserver	7.2	All	All	All
Application	Citrix	Xenserver	6.0.2	All	All	All
Application	Citrix	Xenserver	6.2.0	All	All	All
Application	Citrix	Xenserver	6.5	All	All	All
Application	Citrix	Xenserver	7.0	All	All	All
Application	Citrix	Xenserver	7.1	All	All	All
Application	Citrix	Xenserver	7.2	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Xen	Xen	4.6.0	All	All	All

Operating System	Xen	Xen	4.6.1	All	All	All
Operating System	Xen	Xen	4.6.3	All	All	All
Operating System	Xen	Xen	4.6.4	All	All	All
Operating System	Xen	Xen	4.6.5	All	All	All
Operating System	Xen	Xen	4.6.6	All	All	All
Operating System	Xen	Xen	4.7.0	All	All	All
Operating System	Xen	Xen	4.7.1	All	All	All
Operating System	Xen	Xen	4.7.2	All	All	All
Operating System	Xen	Xen	4.7.3	All	All	All
Operating System	Xen	Xen	4.8.0	All	All	All
Operating System	Xen	Xen	4.8.1	All	All	All
Operating System	Xen	Xen	4.9.0	All	All	All
Operating System	Xen	Xen	4.6.0	All	All	All
Operating System	Xen	Xen	4.6.1	All	All	All
Operating System	Xen	Xen	4.6.3	All	All	All
Operating System	Xen	Xen	4.6.4	All	All	All
Operating System	Xen	Xen	4.6.5	All	All	All
Operating System	Xen	Xen	4.6.6	All	All	All
Operating System	Xen	Xen	4.7.0	All	All	All
Operating System	Xen	Xen	4.7.1	All	All	All
Operating System	Xen	Xen	4.7.2	All	All	All
Operating System	Xen	Xen	4.7.3	All	All	All
Operating System	Xen	Xen	4.8.0	All	All	All
Operating System	Xen	Xen	4.8.1	All	All	All
Operating System	Xen	Xen	4.9.0	All	All	All

References

Reference
Xen Grant Table Allocator Race Condition Lets Local Users on a Guest System Gain Elevated Privileges on the Host System - SecurityTracke
1477651 – (CVE-2017-12136, xsa228) CVE-2017-12136 xsa228 xen: grant_table: Race conditions with maptrack free list handling (XSA-228)
Xen CVE-2017-12136 Privilege Escalation Vulnerability
Xen: Multiple vulnerabilities (GLSA 201801-14) — Gentoo security
XSA-228 - Xen Security Advisories
Citrix XenServer Multiple Security Updates
Debian -- Security Information -- DSA-3969-1 xen

oss-security - Xen Security Advisory 228 (CVE-2017-12136) - grant_table: Race conditions with maptrack free list handling

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500817 Alpine Linux Security Update for xen

504560 Alpine Linux Security Update for xen

710266 Gentoo Linux Xen Multiple Vulnerabilities (GLSA 201801-14)