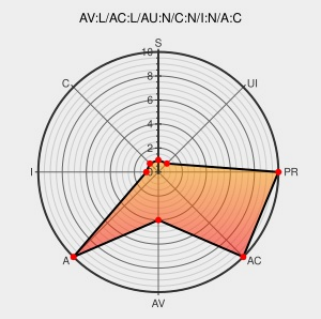
CVE-2015-7970

Published on: 10/30/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:12 PM UTC

CVE-2015-7970

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Xen from Xen contain the following vulnerability:

The p2m_pod_emergency_sweep function in arch/x86/mm/p2m-pod.c in Xen 3.4.x, 3.5.x, and 3.6.x is not preemptible, which allows local x86 HVM guest administrators to cause a denial of service (CPU consumption and possibly reboot) via crafted memory contents that triggers a "time-consuming linear scan," related to Populate-on-Demand.

CVE-2015-7970 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Xen Populate-on-Demand Mode Memory Error Lets Local Users on a Guest System Cause Denial of Service Conditions on the Host System - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1034034
404 - Page not found	support.citrix.com text/html	CONFIRM support.citrix.com/article/CTX202404
[SECURITY] Fedora 21 Update: xen-4.4.3-7.fc21	lists.fedoraproject.org text/html	FEDORA FEDORA-2015-242be2c240
[SECURITY] Fedora 23 Update: xen-4.5.1-14.fc23	lists.fedoraproject.org text/html	FEDORA FEDORA-2015-a931b02be2
Xen CVE-2015-7970 Local Denial of Service Vulnerability	cve.report (archive) text/html	BID 77362

XSA-150 - Xen Security Advisories	Vendor Advisory xenbits.xen.org text/html	CONFIRM xenbits.xen.org/xsa/advisory-150.html
openSUSE-SU-2015:2250-1: moderate: Security update for xen	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:2250
Debian -- Security Information -- DSA-3414-1 xen	www.debian.org Depreciated Link text/html	DEBIAN DSA-3414
Xen: Multiple vulnerabilities (GLSA 201604-03) — Gentoo Security	security.gentoo.org text/html	GENTOO GLSA-201604-03
[SECURITY] Fedora 22 Update: xen-4.5.1-14.fc22	lists.fedoraproject.org text/html	FEDORA FEDORA-2015-6f6b79efe2

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	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

cpe:2.3:o:xen:xen:3.4.0:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:3.4.1:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:3.4.2:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:3.4.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.4:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:3.4.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→