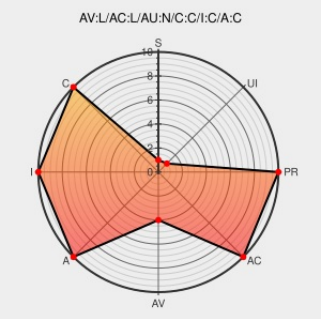
CVE-2015-8338

Published on: 12/17/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:13 PM UTC

CVE-2015-8338

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



Certain versions of Xen from Xen contain the following vulnerability:

Xen 4.6.x and earlier does not properly enforce limits on page order inputs for the (1) XENMEM_increase_reservation, (2) XENMEM_populate_physmap, (3) XENMEM_exchange, and possibly other HYPERVISOR_memory_op suboperations, which allows ARM guest OS administrators to cause a denial of service (CPU consumption, guest reboot, or watchdog timeout and host reboot) and possibly have unspecified other impact via unknown vectors.

CVE-2015-8338 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
XSA-158 - Xen Security Advisories	Vendor Advisory, xenbits.xen.org, text/html	CONFIRM xenbits.xen.org/xsa/advisory-158.html
Xen HYPERVISOR_memory_op Missing Resource Limits Let Local Administrative Users on a Guest System Cause Denial of Service Conditions on the Host System - SecurityTracker	www.securitytracker.com, text/html	SECTRACK 1034390
Debian -- Security Information -- DSA-3633-1 xen	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-3633
Xen CVE-2015-8338 Denial of Service Vulnerability	cve.report (archive), text/html	BID 78920

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	All	All	All	All

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→