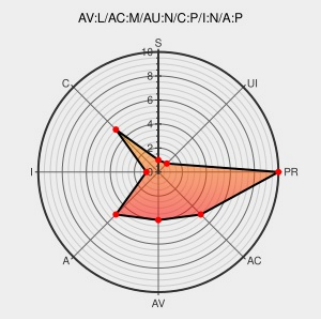
CVE-2014-3717

Published on: 05/19/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:46 PM UTC

CVE-2014-3717

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



Certain versions of Xen from Xen contain the following vulnerability:

Xen 4.4.x does not properly validate the load address for 64-bit ARM guest kernels, which allows local users to read system memory or cause a denial of service (crash) via a crafted kernel, which triggers a buffer overflow.

CVE-2014-3717 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 3.3 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	PARTIAL

CVE References

Description	Tags	Link
oss-security - Xen Security Advisory 95 - input handling vulnerabilities loading guest kernel on ARM	Mailing List, Third Party Advisory, www.openwall.com, text/html	MLIST [oss-security] 20140514 Xen Security Advisory 95 - input handling vulnerabilities loading guest kernel on ARM
oss-security - Re: Xen Security Advisory 95 - input handling vulnerabilities loading guest kernel on ARM	Mailing List, Third Party Advisory, www.openwall.com, text/html	MLIST [oss-security] 20140515 Re: Xen Security Advisory 95 - input handling vulnerabilities loading guest kernel on ARM
XSA-95 - Xen Security Advisories	Patch, Vendor Advisory, xenbits.xen.org, text/html	CONFIRM xenbits.xen.org/xsa/advisory-95.html
oss-security - Xen Security Advisory 95 (CVE-2014-3714 CVE-2014-3715 CVE-2014-3716 CVE-2014-3717) -	Mailing List, Third Party Advisory	MLIST [oss-security] 20140516 Xen Security Advisory 95 (CVE-2014-3714 CVE-2014-

input handling vulnerabilities loading guest kernel on ARM	Third Party Advisory www.openwall.com text/html	Advisory 66 (CVE-2014-3714,CVE-2014-3715,CVE-2014-3716,CVE-2014-3717) - input handling vulnerabilities loading guest kernel on ARM
Xen ARM Guest Loading Bugs Let Local Users Deny Service - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1030252

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	4.4.0	All	All	All
Operating System	Xen	Xen	4.4.0	rc1	All	All
Operating System	Xen	Xen	4.4.0	All	All	All
Operating System	Xen	Xen	4.4.0	rc1	All	All

cpe:2.3:o:xen:xen:4.4.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.4.0:rc1:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.4.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.4.0:rc1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→