

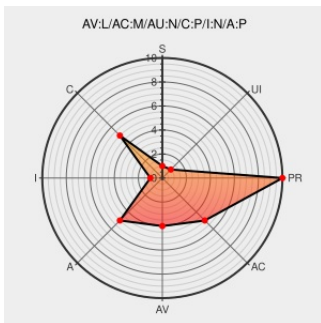


CVE-2014-3714

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

Last Modified on: 03/23/2021 11:25:47 PM UTC

CVE-2014-3714

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Xen](#) from [Xen](#) contain the following vulnerability:

The ARM image loading functionality in Xen 4.4.x does not properly validate kernel length, which allows local users to read system memory or cause a denial of service (crash) via a crafted 32-bit ARM guest kernel in an image, which triggers a buffer overflow.

CVE-2014-3714 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **3.3 - LOW**

**Access
Vector**

LOCAL

**Access
Complexity**

MEDIUM

Authentication

NONE

**Confidentiality
Impact**

PARTIAL

**Integrity
Impact**

NONE

**Availability
Impact**

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-](#)

CVE-2014-3715,CVE-2014-3716,CVE-2014-3717) - input handling vulnerabilities loading guest kernel on ARM

Third Party Advisory
www.openwall.com
text/html

SECURITY SC (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

SECTRAK 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→