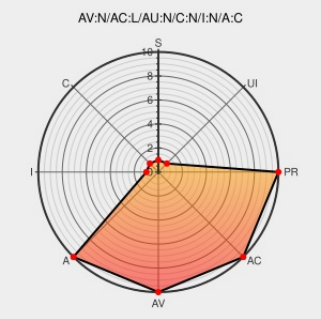
CVE-2015-8341

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

Last Modified on: 03/23/2021 11:26:14 PM UTC

CVE-2015-8341

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



Certain versions of Xen from Xen contain the following vulnerability:

The libxl toolstack library in Xen 4.1.x through 4.6.x does not properly release mappings of files used as kernels and initial ramdisks when managing multiple domains in the same process, which allows attackers to cause a denial of service (memory and disk consumption) by starting domains.

CVE-2015-8341 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-3519-1 xen	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-3519
Xen libxl Error Conditions Let Local Users on a Guest System Cause Denial of Service Conditions on the Host System - SecurityTracker	www.securitytracker.com, text/html	SECTRACK 1034389
Xen: Multiple vulnerabilities (GLSA 201604-03) — Gentoo Security	security.gentoo.org, text/html	GENTOO GLSA-201604-03
XSA-160 - Xen Security Advisories	Vendor Advisory, xenbits.xen.org, text/html	CONFIRM xenbits.xen.org/xsa/advisory-160.html

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	4.1.0	All	All	All
Operating System	Xen	Xen	4.1.1	All	All	All
Operating System	Xen	Xen	4.1.2	All	All	All
Operating System	Xen	Xen	4.1.3	All	All	All
Operating System	Xen	Xen	4.1.4	All	All	All
Operating System	Xen	Xen	4.1.5	All	All	All
Operating System	Xen	Xen	4.1.6	All	All	All
Operating System	Xen	Xen	4.1.6.1	All	All	All
Operating System	Xen	Xen	4.2.0	All	All	All
Operating System	Xen	Xen	4.2.1	All	All	All
Operating System	Xen	Xen	4.2.2	All	All	All
Operating System	Xen	Xen	4.2.3	All	All	All
Operating System	Xen	Xen	4.2.4	All	All	All
Operating System	Xen	Xen	4.2.5	All	All	All
Operating System	Xen	Xen	4.3.0	All	All	All
Operating System	Xen	Xen	4.3.1	All	All	All
Operating System	Xen	Xen	4.3.2	All	All	All
Operating System	Xen	Xen	4.3.3	All	All	All
Operating System	Xen	Xen	4.3.4	All	All	All

Operating System	Xen	Xen	4.4.0	All	All	All
Operating System	Xen	Xen	4.4.1	All	All	All
Operating System	Xen	Xen	4.4.2	All	All	All
Operating System	Xen	Xen	4.4.3	All	All	All
Operating System	Xen	Xen	4.5.0	All	All	All
Operating System	Xen	Xen	4.5.1	All	All	All
Operating System	Xen	Xen	4.5.2	All	All	All
Operating System	Xen	Xen	4.6.0	All	All	All
Operating System	Xen	Xen	4.1.0	All	All	All
Operating System	Xen	Xen	4.1.1	All	All	All
Operating System	Xen	Xen	4.1.2	All	All	All
Operating System	Xen	Xen	4.1.3	All	All	All
Operating System	Xen	Xen	4.1.4	All	All	All
Operating System	Xen	Xen	4.1.5	All	All	All
Operating System	Xen	Xen	4.1.6	All	All	All
Operating System	Xen	Xen	4.1.6.1	All	All	All
Operating System	Xen	Xen	4.2.0	All	All	All
Operating System	Xen	Xen	4.2.1	All	All	All
Operating System	Xen	Xen	4.2.2	All	All	All
Operating System	Xen	Xen	4.2.3	All	All	All
Operating System	Xen	Xen	4.2.4	All	All	All
Operating System	Xen	Xen	4.2.5	All	All	All
Operating System	Xen	Xen	4.3.0	All	All	All

Operating System	Xen	Xen	4.3.1	All	All	All
Operating System	Xen	Xen	4.3.2	All	All	All
Operating System	Xen	Xen	4.3.3	All	All	All
Operating System	Xen	Xen	4.3.4	All	All	All
Operating System	Xen	Xen	4.4.0	All	All	All
Operating System	Xen	Xen	4.4.1	All	All	All
Operating System	Xen	Xen	4.4.2	All	All	All
Operating System	Xen	Xen	4.4.3	All	All	All
Operating System	Xen	Xen	4.5.0	All	All	All
Operating System	Xen	Xen	4.5.1	All	All	All
Operating System	Xen	Xen	4.5.2	All	All	All
Operating System	Xen	Xen	4.6.0	All	All	All

cpe:2.3:o:xen:xen:4.1.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.4:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.5:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.6:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.6.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.4:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.5:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.4:*:*:*:*:*:*:*:

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

cpe:2.3:o:xen:xen:4.4.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.4.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.4.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.5.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.5.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.5.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.6.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.4:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.5:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.6:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.1.6.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.1:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.2:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.3:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.4:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.2.5:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.0:*:*:*:*:*:*:*:

cpe:2.3:o:xen:xen:4.3.1:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.3.2:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.3.3:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.3.4:*:*:*:*:*:*:*

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

cpe:2.3:o:xen:xen:4.4.1:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.4.2:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.4.3:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.5.0:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.5.1:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.5.2:*:*:*:*:*:*:*

cpe:2.3:o:xen:xen:4.6.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→