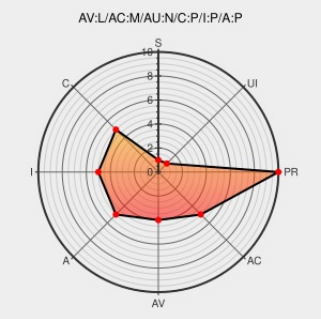
CVE-2013-4371

Published on: 10/17/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:08:13 AM UTC

CVE-2013-4371

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



Certain versions of Xen from Xen contain the following vulnerability:

Use-after-free vulnerability in the libxl_list_cpupool function in the libxl toolstack library in Xen 4.2.x and 4.3.x, when running "under memory pressure," returns the original pointer when the realloc function fails, which allows local users to cause a denial of service (heap corruption and crash) and possibly execute arbitrary code via unspecified vectors.

CVE-2013-4371 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4.4 - MEDIUM

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

CVE References

Description	Tags	Link
Gentoo Linux Documentation -- Xen: Multiple Vunlerabilities	security.gentoo.org text/html	GENTOO GLSA-201407-03
oss-security - Xen Security Advisory 70 (CVE-2013-4371) - use-after-free in libxl_list_cpupool under memory pressure	www.openwall.com text/html	MLIST [oss-security] 20131010 Xen Security Advisory 70 (CVE-2013-4371) - use-after-free in libxl_list_cpupool under memory pressure

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	4.2.0	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	4.3.0	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	4.3.0	All	All	All

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:4.3.0:*:*:*:*:*:*:*:

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:4.3.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report