



CVE-2013-4371

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

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

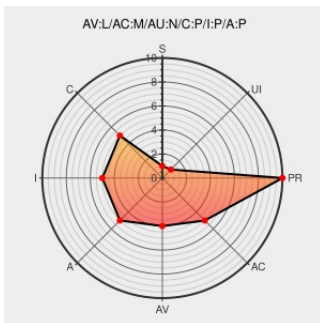
CVE-2013-4371

[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

LOCAL

Access Complexity

MEDIUM

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

PARTIAL

Availability Impact

PARTIAL

CVE References

Description

Tags

Link

Gentoo Linux Documentation -- Xen: Multiple Vulnerabilities

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](#)

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	4.2.0	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

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)