



CVE-2021-28705

Published on: 11/23/2021 12:00:00 AM UTC

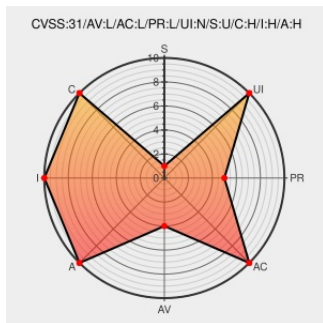
Last Modified on: 12/01/2021 07:15:00 AM UTC

CVE-2021-28705

Source: Mitre

Source: Nist

Print: PDF



Certain versions of Xen from Xen contain the following vulnerability:

issues with partially successful P2M updates on x86 T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] x86 HVM and PVH guests may be started in populate-on-demand (PoD) mode, to provide a way for them to later easily have more memory assigned. Guests are permitted to control certain P2M aspects of individual pages via

hypercalls. These hypercalls may act on ranges of pages specified via page orders (resulting in a power-of-2 number of pages). In some cases the hypervisor carries out the requests by splitting them into smaller chunks. Error handling in certain PoD cases has been insufficient in that in particular partial success of some operations was not properly accounted for. There are two code paths affected - page removal (CVE-2021-28705) and insertion of new pages (CVE-2021-28709). (We provide one patch which combines the fix to both issues.)

CVE-2021-28705 has been assigned by security@xen.org to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: Xen - xen version 4.14.x

Affected Vendor/Software: Xen - xen version 4.12.x

Affected Vendor/Software: Xen - xen version 4.15.x

Affected Vendor/Software: Xen - xen version xen-unstable

Affected Vendor/Software: Xen - xen version 4.13.x

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.9 - MEDIUM**

Access Vector

Access Complexity

Authentication

LOCAL

MEDIUM

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description

Tags

Link

[xenbits.xenproject.org](https://xenbits.xenproject.org/text/plain)
[text/plain](#)

 **MISC**
xenbits.xenproject.org/xsa/advisory-389.txt

[SECURITY] Fedora 35 Update: xen-4.15.1-4.fc35 - package-announce - Fedora Mailing-Lists

[lists.fedoraproject.org](https://lists.fedoraproject.org/text/html)
[text/html](#)

 **FEDORA FEDORA-2021-03645e9807**

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.

Related QID Numbers

[751411](#) SUSE Enterprise Linux Security Update for xen (SUSE-SU-2021:3852-1)

[751414](#) SUSE Enterprise Linux Security Update for xen (SUSE-SU-2021:3851-1)

[751417](#) SUSE Enterprise Linux Security Update for xen (SUSE-SU-2021:3842-1)

[751422](#) SUSE Enterprise Linux Security Update for xen (SUSE-SU-2021:3849-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Xen	Xen	4.15.0	All	All	All
Operating System	Xen	Xen	4.15.1	All	All	All
Operating System	Xen	Xen	All	All	All	All
Operating System	Xen	Xen	All	All	All	All
Operating System	Xen	Xen	All	All	All	All

`cpe:2.3:o:xen:xen:4.15.0:*:*:*:*:x86:*`

`cpe:2.3:o:xen:xen:4.15.1:*:*:*:*:x86:*`

cpe:2.3:o:xen:xen:*****:x86:*
cpe:2.3:o:xen:xen:*****:x86:*
cpe:2.3:o:xen:xen:*****:x86:*

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-28705 : issues with partially successful P2M updates on x86 T[his CNA information record relates to multi... twitter.com/i/web/status/1...	2021-11-24 01:08:39
 @oss_security	Xen Security Advisory 389 v3 (CVE-2021-28705,CVE-2021-28709) - issues with partially successful P2M updates on x86:... twitter.com/i/web/status/1...	2021-11-24 02:30:11

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021   |

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