



CVE-2021-28707

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

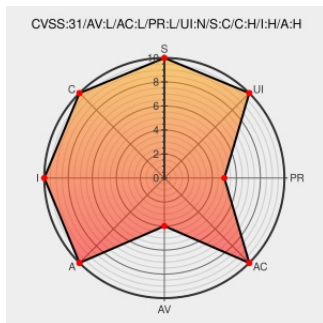
Last Modified on: 12/01/2021 07:59:00 AM UTC

CVE-2021-28707

Source: Mitre

Source: Nist

Print: PDF



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

PoD operations on misaligned GFNs 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). The implementation of some of these hypercalls for PoD does not enforce the base page frame number to be suitably aligned for the specified order, yet some code involved in PoD handling actually makes such an assumption. These operations are XENMEM_decrease_reservation (CVE-2021-28704) and XENMEM_populate_physmap (CVE-2021-28707), the latter usable only by domains controlling the guest, i.e. a de-privileged gemu or a stub domain. (Patch 1, combining the fix to both these two issues.) In addition handling of XENMEM_decrease_reservation can also trigger a host crash when the specified page order is neither 4k nor 2M nor 1G (CVE-2021-28708, patch 2).

CVE-2021-28707 has been assigned by security@xen.org to track the vulnerability - currently rated as **HIGH** severity.

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

Affected Vendor/Software: Xen - xen version ?< 4.12

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

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

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

CVSS3 Score: **8.8 - HIGH**

Attack Vector

Attack Complexity

Privileges Required

User Interaction

LOCAL



LOW

LOW

NONE

Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	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
[SECURITY] Fedora 35 Update: xen-4.15.1-4.fc35 - package-announce - Fedora Mailing-Lists	Mailing List Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2021-03645e9807
	xenbits.xenproject.org text/plain	 MISC xenbits.xenproject.org/xsa/advisory-388.txt

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	All	All	All	All
cpe:2.3:o:xen:xen:*:*:*:*:*:x86.*:						

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-28707 : PoD operations on misaligned GFNs T[his CNA information record relates to multiple CVEs; the text... twitter.com/i/web/status/1...	2021-11-24 01:00:35



@oss_security

Xen Security Advisory 388 v3 (CVE-2021-28704,CVE-2021-28707,CVE-2021-28708) - PoD operations on misaligned GFNs: Po... twitter.com/i/web/status/1...

2021-11-24
02:30:14

[← 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