



CVE-2019-19581

Published on: 12/11/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:54 PM UTC

CVE-2019-19581

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H



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

An issue was discovered in Xen through 4.12.x allowing 32-bit Arm guest OS users to cause a denial of service (out-of-bounds access) because certain bit iteration is mishandled. In a number of places bitmaps are being used by the hypervisor to track certain state.

Iteration over all bits involves functions which may misbehave in certain corner cases: On 32-bit Arm accesses to bitmaps with bit a count which is a multiple of 32, an out of bounds access may occur. A malicious guest may cause a hypervisor crash or hang, resulting in a Denial of Service (DoS). All versions of Xen are vulnerable. 32-bit Arm systems are vulnerable. 64-bit Arm systems are not vulnerable.

CVE-2019-19581 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-4602-1 xen	www.debian.org Depreciated Link text/html	 DEBIAN DSA-4602
Xen: Multiple vulnerabilities (GLSA 202003-56) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-202003-56
[SECURITY] Fedora 31 Update: xen-4.12.1-8.fc31 - package-announce - Fedora Mailing-Lists	Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2019-6aad703290
[SECURITY] Fedora 30 Update: xen-4.11.3-2.fc30 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2019-2e12bd3a9a
XSA-307 - Xen Security Advisories	Patch Vendor Advisory xenbits.xen.org text/html	 MISC xenbits.xen.org/xsa/advisory-307.html
[security-announce] openSUSE-SU-2020:0011-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2020:0011
Bugtraq: [SECURITY] [DSA 4602-1] xen security update	seclists.org text/html	 BUGTRAQ 20200114 [SECURITY] [DSA 4602-1] xen security update

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	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Xen	Xen	All	All	All	All
cpe:2.3:o:fedoraproject:fedora:31:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:31:*:*:*:*:*:						
cpe:2.3:o:xen:xen:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [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](#)