

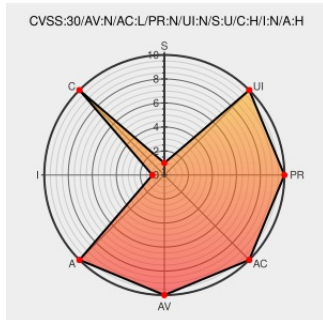


CVE-2019-15753

Published on: 08/28/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:44 PM UTC

CVE-2019-15753

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

Certain versions of [Os-vif](#) from [Openstack](#) contain the following vulnerability:

In OpenStack os-vif 1.15.x before 1.15.2, and 1.16.0, a hard-coded MAC aging time of 0 disables MAC learning in linuxbridge, forcing obligatory Ethernet flooding of non-local destinations, which both impedes network performance and allows users to possibly view the content of packets for instances belonging to other tenants sharing the same network. Only deployments using the linuxbridge backend are affected. This occurs in `PyRoute2.add()` in `internal/command/ip/linux/impl_pyroute2.py`.

CVE-2019-15753 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.1 - CRITICAL**

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

CVSS2 Score: **6.4 - MEDIUM**

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

CVE References

Description	Tags	Link
bug #1827529 [FOSSA-2019-0041] Aging time of 0	OpenStack	MISC linuxbridge not/bug/1827529

Bug #1837232 [OSSA-2019-004] Ageing time of 0 disables linuxbridge MAC learning : Bugs : os-vif	Issue Tracking Third Party Advisory launchpad.net text/html	 MISC launchpad.net/bugs/1837232
No Description Provided	Patch review.opendev.org text/html	 MISC review.opendev.org/678098
OpenStack Docs: OSSA-2019-004: Ageing time of 0 disables linuxbridge MAC learning	Patch Vendor Advisory security.openstack.org text/html	 CONFIRM security.openstack.org/ossa/OSSA-2019-004.html
No Description Provided	Patch review.opendev.org text/html	 MISC review.opendev.org/672834
oss-security - [OSSA-2019-004] Ageing time of 0 disables linuxbridge MAC learning (CVE-2019-15753)	Mailing List Patch Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20190829 [OSSA-2019-004] Ageing time of 0 disables linuxbridge MAC learning (CVE-2019-15753)

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
Application	Openstack	Os-vif	All	All	All	All
Application	Openstack	Os-vif	1.16.0	All	All	All
Application	Openstack	Os-vif	All	All	All	All
Application	Openstack	Os-vif	1.16.0	All	All	All
cpe:2.3:a:openstack:os-vif:*:*:*:*:*:						
cpe:2.3:a:openstack:os-vif:1.16.0:*:*:*:*:						
cpe:2.3:a:openstack:os-vif:*:*:*:*:*:						
cpe:2.3:a:openstack:os-vif:1.16.0:*:*:*:*:						

No vendor comments have been submitted for this CVE

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](#)