



# CVE-2019-10161

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2019-10161
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-07-30 23:15:00 UTC
<b>Updated</b>	2023-11-07 03:02:00 UTC
<b>Description</b>	It was discovered that libvirt before versions 4.10.1 and 5.4.1 would permit read-only clients to use the virDomainSavelma

## Risk And Classification

**Problem Types:** CWE-22 | CWE-862

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Libvirt</a>	All	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Libvirt</a>	All	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Libvirt</a>	All	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Virtualization</a>	4.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Virtualization Host</a>	4.0	All	All	All

## References

Reference	Source	Link
-----------	--------	------

libvirt: Multiple vulnerabilities (GLSA 202003-18) — Gentoo security	GENTOO	<a href="#">secu</a>
libvirt privilege escalation vulnerabilities - Red Hat Customer Portal	CONFIRM	<a href="#">acce</a>
1720115 – (CVE-2019-10161) CVE-2019-10161 libvirt: arbitrary file read/exec via virDomainSaveImageGetXMLDesc API	CONFIRM	<a href="#">bugz</a>
USN-4047-2: libvirt update vulnerability   Ubuntu security notices   Ubuntu	UBUNTU	<a href="#">usn.</a>
libvirt.org Git - libvirt.git/commit	CONFIRM	<a href="#">libvir</a>
libvirt.org Git - libvirt.git/commit		<a href="#">libvir</a>
CVE Program record	CVE.ORG	<a href="#">www</a>
NVD vulnerability detail	NVD	<a href="#">nvd.</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[377037](#) Alibaba Cloud Linux Security Update for libvirt (ALINUX2-SA-2019:0039)

[377413](#) Alibaba Cloud Linux Security Update for virt:rhel and virt-devel:rhel (ALINUX3-SA-2022:0119)

[378197](#) Virtuozzo Linux Security Update for libvirt-devel (VZLSA-2019:1578)

[500325](#) Alpine Linux Security Update for libvirt

© [CVE.report](#) 2026 |

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](#)