



CVE-2010-2239

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

Summary

CVE	CVE-2010-2239
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-08-19 18:00:00 UTC
Updated	2010-10-30 05:41:00 UTC
Description	Red Hat libvirt, possibly 0.6.0 through 0.8.2, creates new images without setting the user-defined backing-store format, which

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libvirt	Libvirt	0.6.0	All	All	All
Application	Libvirt	Libvirt	0.6.1	All	All	All
Application	Libvirt	Libvirt	0.6.2	All	All	All
Application	Libvirt	Libvirt	0.6.3	All	All	All
Application	Libvirt	Libvirt	0.6.4	All	All	All
Application	Libvirt	Libvirt	0.6.5	All	All	All
Application	Libvirt	Libvirt	0.7.0	All	All	All
Application	Libvirt	Libvirt	0.7.1	All	All	All
Application	Libvirt	Libvirt	0.7.2	All	All	All
Application	Libvirt	Libvirt	0.7.3	All	All	All
Application	Libvirt	Libvirt	0.7.4	All	All	All
Application	Libvirt	Libvirt	0.7.5	All	All	All
Application	Libvirt	Libvirt	0.7.6	All	All	All
Application	Libvirt	Libvirt	0.7.7	All	All	All
Application	Libvirt	Libvirt	0.8.0	All	All	All
Application	Libvirt	Libvirt	0.8.1	All	All	All
Application	Libvirt	Libvirt	0.8.2	All	All	All

Application	Libvirt	Libvirt	0.6.0	All	All	All
Application	Libvirt	Libvirt	0.6.1	All	All	All
Application	Libvirt	Libvirt	0.6.2	All	All	All
Application	Libvirt	Libvirt	0.6.3	All	All	All
Application	Libvirt	Libvirt	0.6.4	All	All	All
Application	Libvirt	Libvirt	0.6.5	All	All	All
Application	Libvirt	Libvirt	0.7.0	All	All	All
Application	Libvirt	Libvirt	0.7.1	All	All	All
Application	Libvirt	Libvirt	0.7.2	All	All	All
Application	Libvirt	Libvirt	0.7.3	All	All	All
Application	Libvirt	Libvirt	0.7.4	All	All	All
Application	Libvirt	Libvirt	0.7.5	All	All	All
Application	Libvirt	Libvirt	0.7.6	All	All	All
Application	Libvirt	Libvirt	0.7.7	All	All	All
Application	Libvirt	Libvirt	0.8.0	All	All	All
Application	Libvirt	Libvirt	0.8.1	All	All	All
Application	Libvirt	Libvirt	0.8.2	All	All	All

References

Reference	Source	Link
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
[SECURITY] Fedora 13 Update: libvirt-0.8.2-1.fc13	FEDORA	lists.fedoraproject.org
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:017	SUSE	lists.opensuse.org
[SECURITY] Fedora 12 Update: libvirt-0.8.2-1.fc12	FEDORA	lists.fedoraproject.org
USN-1008-1: libvirt vulnerabilities Ubuntu	UBUNTU	ubuntu.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
libvirt: Releases	MISC	libvirt.org
Support	REDHAT	www.redhat.com
USN-1008-3: libvirt update Ubuntu	UBUNTU	ubuntu.com
USN-1008-2: Virtinst update Ubuntu	UBUNTU	ubuntu.com
Bug 607812 – CVE-2010-2239 libvirt: not setting user defined backing store format when creating new image	CONFIRM	bugzilla.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)