

159880 Oracle Enterprise Linux Security Update for kvm_utils (ELSA-2022-9460)
160248 Oracle Enterprise Linux Security Update for virt:ol and virt-devel:ol (ELSA-2022-7472)
160281 Oracle Enterprise Linux Security Update for libvirt (ELSA-2022-8003)
184154 Debian Security Update for libvirt (CVE-2022-0897)
198763 Ubuntu Security Notification for libvirt Vulnerabilities (USN-5399-1)
199383 Ubuntu Security Notification for libvirt Vulnerabilities (USN-6126-1)
240837 Red Hat Update for virt:rhel and virt-devel:rhel security (RHSA-2022:7472)
240905 Red Hat Update for libvirt security (RHSA-2022:8003)
6000552 Debian Security Update for libvirt (DLA 3778-1)
710643 Gentoo Linux libvirt Multiple Vulnerabilities (GLSA 202210-06)
752105 SUSE Enterprise Linux Security Update for libvirt (SUSE-SU-2022:1540-1)
752107 SUSE Enterprise Linux Security Update for libvirt (SUSE-SU-2022:1549-1)
754151 SUSE Enterprise Linux Security Update for libvirt (SUSE-SU-2023:2754-1)
940828 AlmaLinux Security Update for libvirt (ALSA-2022:8003)
960170 Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2022:7472)
960643 Rocky Linux Security Update for libvirt (RLSA-2022:8003)

© [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](#)