Lumeta CVE Radar 4.5

CentOS Linux—the open, enterprise-class, platform upon which Lumeta solutions are built—and third-party packages such as Postgres and Oracle JRE—are continuously monitored by industry and community groups to uncover flaws. Upgrade packages that fix these CentOS flaws (aka CVEs, Common Vulnerabilities and Exposures) are made available from CentOS and third parties (Postgres, Oracle JRE) on an ongoing basis.

This page lists security enhancements on our radar. It's those CVEs that Lumeta is actively addressing and expects to have fully resolved in the upcoming releases of Lumeta Enterprise Edition.

CVE	Repair	Date	3rd Party Patch	Vulnerability		Resolved_Version & GA Date	
Identifier	**PKG**	**Reported**	**Available?**	**Lumeta**	**Notes on vulnerability**	**Lumeta**	**Lumeta_GA**
CVE-2021-45417	aide-0.15.1-13.el7_9.1.x86_64		CentOS yes	yes	A heap-based buffer overflow vulnerability in the base64 functions of AIDE, an advanced intrusion detection system. An attacker could crash the program and possibly execute arbitrary code through large (<16k) extended file attributes or ACL. https://access.redhat.com/security/cve/cve-2021-45417	4.5.0.0	5/27/2022
CVE-2022-22823	expat-2.1.0-14.el7_9.x86_64		CentOS yes	yes	expat (libexpat) is susceptible to a software flaw that causes process interruption. When processing a large number of prefixed XML attributes on a single tag can libexpat can terminate unexpectedly due to integer overflow. The highest threat from this vulnerability is to availability, confidentiality and integrity. https://access.redhat.com/security/cve/cve-2022-22823	4.5.0.0	5/27/2022
CVE-2022-22824	expat-2.1.0-14.el7_9.x86_64		CentOS yes	yes	expat (libexpat) is susceptible to a software flaw that causes process interruption. When processing numerous prefixed XML attributes on a single tag can libexpat can terminate unexpectedly due to integer overflow. The highest threat from this vulnerability is to availability, confidentiality, and integrity. https://access.redhat.com/security/cve/cve-2022-22824	4.5.0.0	5/27/2022
CVE-2022-22827	expat-2.1.0-14.el7_9.x86_64		CentOS yes	yes	expat (libexpat) is susceptible to a software flaw that causes process interruption. When processing a large number of prefixed XML attributes on a single tag can libexpat can terminate unexpectedly due to integer overflow. The highest threat from this vulnerability is to availability, confidentiality and integrity. https://access.redhat.com/security/cve/cve-2022-22827	4.5.0.0	5/27/2022
CVE-2022-25315	expat-2.1.0-14.el7_9.x86_64		CentOS yes	yes	An integer overflow was found in expat. The issue occurs in storeRawNames() by abusing the m_buffer expansion logic to allow allocations very close to INT_MAX and out-of-bounds heap writes. This flaw can cause a denial of service or potentially arbitrary code execution. https://access.redhat.com/security/cve/cve-2020-11668	4.5.0.0	5/27/2022
CVE-2021-22555	kernel-3.10.0-1160.59.1.el7.x86_64		CentOS yes	yes	A flaw was discovered in processing setsockopt IPT_SO_SET_REPLACE (or IP6T_SO_SET_REPLACE) for 32 bit processes on 64 bit systems. This flaw will allow local user to gain privileges or cause a DoS through user name space. This action is usually restricted to root-privileged users but can also be leveraged if the kernel is compiled with CONFIG_USER_NS and CONFIG_NET_NS and the user is granted elevated privileges. https://access.redhat.com/security/cve/cve-2021-22555	4.5.0.0	5/27/2022
CVE-2021-3656	kernel-tools-3.10.0-1160.59.1.el7.x86_64		CentOS yes	yes	A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "virt_ext" field, this issue could allow a malicious L1 to disable both VMLOAD /VMSAVE intercepts and VLS (Virtual VMLOAD/VMSAVE) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape. https://access.redhat.com/security/cve/cve-2021-3656	4.5.0.0	5/27/2022