



# CVE-2023-4641

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

## Summary

<b>CVE</b>	CVE-2023-4641
<b>State</b>	RESERVED
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-12-27 16:15:00 UTC
<b>Updated</b>	2024-01-04 17:06:00 UTC
<b>Description</b>	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new

## Risk And Classification

**Problem Types: CWE-287**

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Redhat</a>	<a href="#">Codeready Linux Builder</a>	8.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Codeready Linux Builder</a>	9.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Codeready Linux Builder For Arm64</a>	8.0_aarch64	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Codeready Linux Builder For Arm64</a>	9.0_aarch64	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Codeready Linux Builder For Ibm Z Systems</a>	8.0_s390x	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Codeready Linux Builder For Ibm Z Systems</a>	9.0_s390x	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Codeready Linux Builder For Power Little Endian</a>	8.0_ppc64le	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Codeready Linux Builder For Power Little Endian</a>	9.0_ppc64le	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>	9.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Arm 64</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Arm 64</a>	9.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Ibm Z Systems</a>	8.0_s390x	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Ibm Z Systems</a>	9.0_s390x	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian</a>	8.0_ppc64le	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian</a>	9.0_ppc64le	All	All	All
Application	<a href="#">Shadow-maint</a>	<a href="#">Shadow-utils</a>	All	All	All	All

## References

Reference	Source	Link	Tags
<a href="https://access.redhat.com/security/cve/CVE-2023-4641">access.redhat.com/security/cve/CVE-2023-4641</a>		<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
<a href="#">RHBZ#2215945</a>		<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	Issue Tracking
<a href="#">RHSA-2023:6632</a>		<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
<a href="#">RHSA-2023:7112</a>		<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">161088</a> Oracle Enterprise Linux Security Update for shadow-utils (ELSA-2023-6632)
<a href="#">161164</a> Oracle Enterprise Linux Security Update for shadow-utils (ELSA-2023-7112)
<a href="#">200119</a> Ubuntu Security Notification for shadow Vulnerability (USN-6640-1)
<a href="#">242327</a> Red Hat Update for shadow-utils (RHSA-2023:6632)
<a href="#">242437</a> Red Hat Update for shadow-utils (RHSA-2023:7112)
<a href="#">242854</a> Red Hat Update for shadow-utils (RHSA-2024:0417)
<a href="#">356145</a> Amazon Linux Security Advisory for shadow-utils : ALAS2-2023-2247
<a href="#">356551</a> Amazon Linux Security Advisory for shadow-utils : ALAS-2023-1873
<a href="#">356895</a> Amazon Linux Security Advisory for shadow-utils : ALAS2023-2023-450
<a href="#">356977</a> Amazon Linux Security Advisory for shadow-utils : AL2012-2023-461
<a href="#">379633</a> Alibaba Cloud Linux Security Update for shadow-utils (ALINUX3-SA-2024:0041)
<a href="#">673538</a> EulerOS Security Update for shadow (EulerOS-SA-2023-3350)
<a href="#">673650</a> EulerOS Security Update for shadow (EulerOS-SA-2023-3020)
<a href="#">673701</a> EulerOS Security Update for shadow (EulerOS-SA-2023-3196)
<a href="#">673795</a> EulerOS Security Update for shadow (EulerOS-SA-2023-3043)
<a href="#">673849</a> EulerOS Security Update for shadow-utils (EulerOS-SA-2024-1298)
<a href="#">673883</a> EulerOS Security Update for shadow (EulerOS-SA-2023-3231)
<a href="#">674083</a> EulerOS Security Update for shadow (EulerOS-SA-2023-3318)

<a href="#">755054</a> SUSE Enterprise Linux Security Update for shadow (SUSE-SU-2023:4025-1)
<a href="#">755055</a> SUSE Enterprise Linux Security Update for shadow (SUSE-SU-2023:4024-1)
<a href="#">755056</a> SUSE Enterprise Linux Security Update for shadow (SUSE-SU-2023:4023-1)
<a href="#">755064</a> SUSE Enterprise Linux Security Update for shadow (SUSE-SU-2023:4027-1)
<a href="#">941409</a> AlmaLinux Security Update for shadow-utils (ALSA-2023:6632)
<a href="#">941436</a> AlmaLinux Security Update for shadow-utils (ALSA-2023:7112)

© [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](#)