



# CVE-2023-6356

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

## Summary

<b>CVE</b>	CVE-2023-6356
<b>State</b>	PUBLISHED
<b>Assigner</b>	Unknown
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-02-07 21:15:00 UTC
<b>Updated</b>	2024-03-12 03:15:00 UTC
<b>Description</b>	Description unavailable.

## Risk And Classification

**Problem Types:** CWE-476

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update
Operating System	Linux	Linux Kernel	-	All
Application	Redhat	Codeready Linux Builder Eus	8.6	All
Application	Redhat	Codeready Linux Builder Eus	9.2	All
Application	Redhat	Codeready Linux Builder Eus For Power Little Endian Eus	8.6_ppc64le	All
Application	Redhat	Codeready Linux Builder Eus For Power Little Endian Eus	9.2_ppc64le	All
Application	Redhat	Codeready Linux Builder For Arm64 Eus	8.6_aarch64	All
Application	Redhat	Codeready Linux Builder For Arm64 Eus	9.2_aarch64	All
Application	Redhat	Codeready Linux Builder For Ibm Z Systems Eus	9.2_s390x	All
Operating System	Redhat	Enterprise Linux	8.0	All
Operating System	Redhat	Enterprise Linux	8.0	All
Operating System	Redhat	Enterprise Linux	9.0	All
Operating System	Redhat	Enterprise Linux Eus	8.6	All
Operating System	Redhat	Enterprise Linux Eus	9.2	All
Operating System	Redhat	Enterprise Linux For Arm 64 Eus	8.6_aarch64	All
Operating System	Redhat	Enterprise Linux For Arm 64 Eus	9.2_aarch64	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	8.6_s390x	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	9.2_s390x	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian Eus</a>	8.6_ppc64le	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Power Little Endian Eus</a>	9.2_ppc64le	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Real Time</a>	9.2	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux For Real Time For Nfv</a>	9.2	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	8.6	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	9.2	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions</a>	8.6_ppc64le	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions</a>	9.2_ppc64le	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	8.6	All
Application	<a href="#">Redhat</a>	<a href="#">Virtualization Host</a>	4.0	All

## References

Reference	Source	Link	Tags
RHSA-2024:1248		<a href="https://access.redhat.com">access.redhat.com</a>	
RHSA-2024:0724		<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
RHSA-2024:0897		<a href="https://access.redhat.com">access.redhat.com</a>	
RHBZ#2254054		<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	Issue Tracking
RHSA-2024:0723		<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
<a href="https://access.redhat.com/security/cve/CVE-2023-6356">access.redhat.com/security/cve/CVE-2023-6356</a>		<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
RHSA-2024:0725		<a href="https://access.redhat.com">access.redhat.com</a>	Third Party Advisory
RHSA-2024:0881		<a href="https://access.redhat.com">access.redhat.com</a>	
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="#">161372</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2024-12169)
<a href="#">161402</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2024-0897)
<a href="#">161417</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2024-1248)
<a href="#">242887</a> Red Hat Update for kernel-rt (RHSA-2024:0725)
<a href="#">242890</a> Red Hat Update for kernel (RHSA-2024:0724)
<a href="#">242908</a> Red Hat Update for kernel (RHSA-2024:0723)
<a href="#">242939</a> Red Hat Update for kernel (RHSA-2024:0897)

242983 Red Hat Update for kernel-rt (RHSA-2024:0881)
243052 Red Hat Update for kernel (RHSA-2024:1248)
284894 Fedora Security Update for kernel (FEDORA-2024-0f89e13079)
285011 Fedora Security Update for kernel (FEDORA-2024-50ab089b1d)
755747 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0469-1)
755750 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0476-1)
755751 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0474-1)
755752 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0478-1)
755753 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0484-1)
755754 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0516-1)
755755 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0515-1)
755756 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0514-1)
755988 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0975-1)
941584 AlmaLinux Security Update for kernel (ALSA-2024:0897)

© [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](#)