



CVE-2023-39191

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

Summary

CVE	CVE-2023-39191
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-04 19:15:00 UTC
Updated	2024-01-25 20:15:00 UTC
Description	An improper input validation flaw was found in the eBPF subsystem in the Linux kernel. The issue occurs due to a lack of p

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	38	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All

References

Reference	Source	Link
Red Hat		access
Red Hat		access
Red Hat		access
2226783 – (CVE-2023-39191, ZDI-CAN-19399) CVE-2023-39191 kernel: eBPF: insufficient stack type checks in dynptr	MISC	bugzilla
Red Hat		access
cve-details	MISC	access
ZDI-23-1489 Zero Day Initiative	MISC	www.z
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

161066 Oracle Enterprise Linux Security Update for kernel (ELSA-2023-6583)

242399 Red Hat Update for kernel security (RHSA-2023:6583)

242734 Red Hat Update for kpatch-patch (RHSA-2024:0381)

242845 Red Hat Update for kernel (RHSA-2024:0448)

242846 Red Hat Update for kernel-rt (RHSA-2024:0439)

356634 Amazon Linux Security Advisory for kernel : ALAS2023-2023-422

6140404 AWS Bottlerocket Security Update for kernel (GHSA-qmff-hxw3-jpv4)

755240 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4375-1)

755249 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4414-1)

755567 SUSE Security Update for the linux kernel (SUSE-SU-2023:4343-1)

756013 SUSE Enterprise Linux Security Update for the Linux Kernel RT (Live Patch 6 for SLE 15 SP5) (SUSE-SU-2024:0986-1)

756014 SUSE Enterprise Linux Security Update for the Linux Kernel RT (Live Patch 1 for SLE 15 SP5) (SUSE-SU-2024:0995-1)

756028 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 2 for SLE 15 SP5) (SUSE-SU-2024:1023-1)

756030 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 6 for SLE 15 SP5) (SUSE-SU-2024:1045-1)

756032 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 0 for SLE 15 SP5) (SUSE-SU-2024:1039-1)

756047 SUSE Enterprise Linux Security Update for the Linux Kernel RT (Live Patch 0 for SLE 15 SP5) (SUSE-SU-2024:1097-1)

907630 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (31150-1)

© [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](#)