



CVE-2020-14351

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

Summary

CVE	CVE-2020-14351
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-03 17:15:00 UTC
Updated	2021-11-04 17:05:00 UTC
Description	A flaw was found in the Linux kernel. A use-after-free memory flaw was found in the perf subsystem allowing a local attacker

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Link
1862849 – (CVE-2020-14351) CVE-2020-14351 kernel: performance counters race condition use-after-free	MISC	bugzilla.redhat.com
[SECURITY] [DLA 2494-1] linux security update	MLIST	lists.debian.org
[SECURITY] [DLA 2483-1] linux-4.19 security update	MLIST	lists.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

198328	Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-4912-1)
239151	Red Hat Update for kernel (RHSA-2021:0856)
239182	Red Hat Update for kernel (RHSA-2021:1028)
239456	Red Hat Update for kernel-rt (RHSA-2021:0774)
257070	CentOS Security Update for kernel (CESA-2021:0856)
353100	Amazon Linux Security Advisory for kernel : ALAC2012-2021-024
353101	Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2021-025
353102	Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2021-026
353133	Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-018
375284	EulerOS Security Update for kernel (EulerOS-SA-2021-1311)
377038	Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2020:0198)
390217	Oracle Managed Virtualization (VM) Server for x86 Security Update for Unbreakable Enterprise kernel (OVMSA-2021-0001)
390234	Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0001)
6140044	AWS Bottlerocket Security Update for kernel (GHSA-g44w-2vcw-48f7)
750376	OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)
750533	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2112-1)
750609	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:1906-1)
750738	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:3326-1)
900040	CBL-Mariner Linux Security Update for kernel 5.4.91
902927	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3651)
905917	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3651-1)
940408	AlmaLinux Security Update for kernel (ALSA-2021:0558)

© 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](#).

