



CVE-2020-27777

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

Summary

CVE	CVE-2020-27777
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-15 17:15:00 UTC
Updated	2023-10-05 14:29:00 UTC
Description	A flaw was found in the way RTAS handled memory accesses in userspace to kernel communication. On a locked down (u

Risk And Classification

Problem Types: CWE-862

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	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	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Redhat	Openshift Container Platform	4.4	All	All	All
Application	Redhat	Openshift Container Platform	4.5	All	All	All
Application	Redhat	Openshift Container Platform	4.6	All	All	All
Application	Redhat	Openshift Container Platform	4.4	All	All	All
Application	Redhat	Openshift Container Platform	4.5	All	All	All
Application	Redhat	Openshift Container Platform	4.6	All	All	All

References

Reference	Source	Link
kernel/git/powerpc/linux.git - The powerpc tree	MISC	git.k
oss-security - Re: Linux kernel: powerpc: RTAS calls can be used to compromise kernel integrity	MISC	www
1900844 - (CVE-2020-27777) CVE-2020-27777 kernel: powerpc: RTAS calls can be used to compromise kernel integrity	MISC	bugz
oss-security - Linux kernel: powerpc: RTAS calls can be used to compromise kernel integrity	MISC	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [159375](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2021-3327)
- [159492](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2021-4356)
- [239603](#) Red Hat Update for kernel (RHSA-2021:3327)
- [239816](#) Red Hat Update for kernel security (RHSA-2021:4356)
- [257109](#) CentOS Security Update for kernel (CESA-2021:3327)
- [375284](#) EulerOS Security Update for kernel (EulerOS-SA-2021-1311)
- [670185](#) EulerOS Security Update for kernel (EulerOS-SA-2021-1684)
- [670269](#) EulerOS Security Update for kernel (EulerOS-SA-2021-1808)
- [750376](#) OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)
- [750428](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0075-1)
- [750434](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0060-1)
- [750488](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2260-1)
- [750508](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2193-1)
- [750518](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2161-1)
- [900040](#) CBL-Mariner Linux Security Update for kernel 5.4.91
- [903436](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3700)
- [906092](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3700-1)
- [940265](#) AlmaLinux Security Update for kernel (ALSA-2021:4356)

© [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](#)