

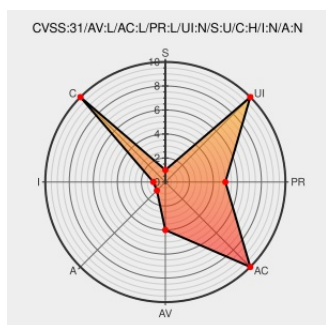


CVE-2021-20269

Published on: Not Yet Published

Last Modified on: 02/12/2023 10:15:00 PM UTC

CVE-2021-20269

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Fedora](#) from [Fedoraproject](#) contain the following vulnerability:

A flaw was found in the permissions of a log file created by kexec-tools. This flaw allows a local unprivileged user to read this file and leak kernel internal information from a previous panic. The highest threat from this vulnerability is to confidentiality. This flaw affects kexec-tools shipped by Fedora versions prior to 2.0.21-8 and RHEL versions prior

to 2.0.20-47.

CVE-2021-20269 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-

1934261 – (CVE-2021-20269) CVE-2021-20269 kexec-tools: incorrect permissions on kdump dmesg file

bugzilla.redhat.com
[text/html](#)

 MISC
bugzilla.redhat.com/show_bug.cgi?id=1934261

Red Hat Customer Portal - Access to 24x7 support and knowledge

access.redhat.com
[text/html](#)

 MISC
access.redhat.com/security/cve/CVE-2021-20269

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[159508](#) Oracle Enterprise Linux Security Update for kexec-tools (ELSA-2021-4404)

[239789](#) Red Hat Update for kexec-tools security (RHSA-2021:4404)

[672258](#) EulerOS Security Update for kexec-tools (EulerOS-SA-2022-2655)

[672304](#) EulerOS Security Update for kexec-tools (EulerOS-SA-2022-2687)

[940219](#) AlmaLinux Security Update for kexec-tools (ALSA-2021:4404)

[960787](#) Rocky Linux Security Update for kexec-tools (RLSA-2021:4404)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	-	All	All	All
Application	Kexec-tools Project	Kexec-tools	All	All	All	All
Application	Kexec-tool Project	Kexec-tool	All	All	All	All
Operating System	Redhat	Enterprise Linux	-	All	All	All
cpe:2.3:o:fedoraproject:fedora:-:*:*:*:*:*:						
cpe:2.3:a:kexec-tools_project:kexec-tools:*:*:*:*:*:*:						
cpe:2.3:a:kexec-tool_project:kexec-tool:*:*:*:*:*:*:						
cpe:2.3:o:redhat:enterprise_linux:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	cve.report/CVE-2021-20269 A flaw was found in the permissions of a log file created by kexec-tools. This flaw allows... twitter.com/i/web/status/1...	2022-03-10 19:16:18



@WesUncensored

New vulnerability on the NVD: CVE-2021-20269 ift.tt/Yg3cmlt

2022-03-10
19:33:12

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)