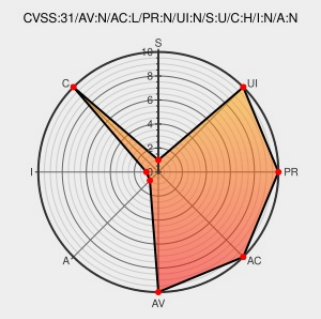
CVE-2021-3714

Published on: Not Yet Published

Last Modified on: 02/12/2023 11:07:00 PM UTC

CVE-2021-3714

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Linux Kernel from Linux contain the following vulnerability:

A flaw was found in the Linux kernels memory deduplication mechanism. Previous work has shown that memory deduplication can be attacked via a local exploitation mechanism. The same technique can be used if an attacker can upload page sized files and detect the change in access time from a networked service to determine if the page has been merged.

CVE-2021-3714 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
	arxiv.org application/pdf	MISC arxiv.org/pdf/2111.08553.pdf
1931327 – (CVE-2021-3714) CVE-2021-3714 kernel: Remote Page Deduplication Attacks	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1931327
[2111.08553] Remote Memory-Deduplication Attacks	arxiv.org text/xml	MISC arxiv.org/abs/2111.08553
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2021-3714

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.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

A flaw was found in the Linux kernels memory deduplication mechanism. Previous work has shown that memory deduplicati…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	-	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

cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:8.0:*:*:*:-:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-3714 : A flaw was found in the #Linux #kernels memory deduplication mechanism. Previous work has shown tha… twitter.com/i/web/status/1…	2022-08-23 16:12:48
/r/netcve	CVE-2021-3714	2022-08-23 17:39:02

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report