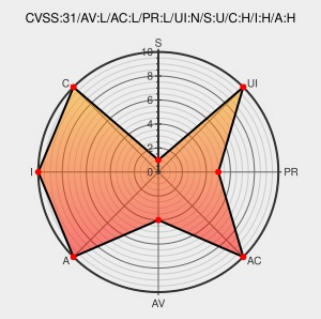
CVE-2021-20226

Published on: 02/23/2021 12:00:00 AM UTC

Last Modified on: 07/28/2023 05:12:00 PM UTC

CVE-2021-20226

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



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

A use-after-free flaw was found in the io_uring in Linux kernel, where a local attacker with a user privilege could cause a denial of service problem on the system The issue results from the lack of validating the existence of an object prior to performing operations on the object by not incrementing the file reference counter while in use. The highest threat from this vulnerability is to data integrity, confidentiality and system availability.

CVE-2021-20226 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 6.1 - MEDIUM

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

CVE References

Description	Tags	Link
CVE-2021-20226 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20210401-

		0001/
1873476 – (CVE-2021-20226) CVE-2021-20226 kernel: use-after-free in io_uring feature	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1873476

Related QID Numbers

179446 Debian Security Update for linux (CVE-2021-20226)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All

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

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

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

cpe:2.3:a:netapp:cloud_backup:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@GrupoICA_Ciber	?LINUX? Múltiples vulnerabilidades de severidad alta en productos LINUX: CVE-2021-28375,CVE-2021-20226 Más info… twitter.com/i/web/status/1…	2021-04-02 08:06:57
@_r_netsec	CVE-2021–20226 a reference counting bug which leads to local privilege escalation in io_uring. flattsecurity.medium.com/cve-2021-20226…	2021-06-21 15:13:06
@netsecu	flattsecurity.medium.com/cve-2021-20226… CVE-2021–20226 a reference counting bug which leads to local privilege escalation in io_uri… twitter.com/i/web/status/1…	2021-06-21 15:50:05
@stereotype32	Linux Kernel Local Privesc (ZDI-2021-001) writeup by @Ga_ryo_ flattsecurity.medium.com/cve-2021-20226… btw I've been doing variou… twitter.com/i/web/status/1…	2021-06-21 16:20:08
@y0n3uchy	A great article on Linux LPE from my colleague .@Ga_ryo_ is out now!? flattsecurity.medium.com/cve-2021-20226…	2021-06-21 16:53:07

@HNTweets	CVE-2021–20226 a reference counting bug which leads to local privilege escalati: flattsecurity.medium.com/cve-2021-20226… Comments: news.ycombinator.com/item?id=275823…	2021-06-21 19:20:03
@winsontang	CVE-2021–20226 a reference counting bug which leads to local privilege escalati flattsecurity.medium.com/cve-2021-20226… https://t.co/uliZYGETen	2021-06-21 19:20:04
@HackerNewsTop10	CVE-2021–20226 a reference counting bug which leads to local privilege escalati Link: flattsecurity.medium.com/cve-2021-20226… Comme… twitter.com/i/web/status/1…	2021-06-21 19:53:59
@newsycombinator	CVE-2021–20226 a reference counting bug which leads to local privilege escalati flattsecurity.medium.com/cve-2021-20226…	2021-06-21 20:02:19
@betterhn20	A reference counting bug which leads to local privilege escalation in io_uring flattsecurity.medium.com/cve-2021-20226… (news.ycombinator.com/item?id=275823…)	2021-06-21 20:27:11
@newsycombinator	A reference counting bug which leads to local privilege escalation in io_uring flattsecurity.medium.com/cve-2021-20226…	2021-06-21 21:01:50
@hackernewsj	io_uringでローカル権限昇格につながる参照カウントのバグ flattsecurity.medium.com/cve-2021-20226…	2021-06-21 22:23:14
@betterhn50	A reference counting bug which leads to local privilege escalation in io_uring flattsecurity.medium.com/cve-2021-20226… (news.ycombinator.com/item?id=275823…)	2021-06-21 22:34:59
@thecat	後來問了強者朋友終於確認 io_uring 後半段唸法比較接近 "而靈" 不是 "幽靈" 啦~? flattsecurity.medium.com/cve-2021-20226…	2021-06-21 23:45:19
@yogishbaliga	#security #software flattsecurity.medium.com/cve-2021-20226…	2021-06-22 01:21:32
@M157q_News_RSS	A reference counting bug which leads to local privilege escalation in io_uring flattsecurity.medium.com/cve-2021-20226… Article URL:… twitter.com/i/web/status/1…	2021-06-22 03:46:05
@HackerNews100	A reference counting bug which leads to local privilege escalation in io_uring flattsecurity.medium.com/cve-2021-20226…	2021-06-22 04:00:20
@W3BGUY	CVE-2021–20226 a reference counting bug which leads to local privilege escalation in io_uring flattsecurity.medium.com/cve-2021-20226…	2021-06-22 13:41:58
@WilfridBlanc	#CVE-202120226 a reference counting bug which leads to local privilege escalation in io_uring. flattsecurity.medium.com/cve-2021-20226…	2021-06-22 14:00:04
@antitree	CVE-2021-20226: io_uring is going to do some potentially cool stuff in the future but today there's a priv esc via… twitter.com/i/web/status/1…	2021-06-22 14:01:00
@hardenedlinux	flattsecurity.medium.com/cve-2021-20226…	2021-07-05 12:07:56
@reverseame	CVE-2021–20226 a reference counting bug which leads to local privilege escalation in io_uring flattsecurity.medium.com/cve-2021-20226…	2021-07-13 06:17:34
@chompie1337	A great example of this in io_uring by @Ga_ryo_ flattsecurity.medium.com/cve-2021-20226… twitter.com/tehjh/status/1…	2021-08-25 20:38:08
@flatt_security	また、ZDI-21-001として公開していた実績をCVE-2021-20226へとアップデートしました。 合わせてreferenceにブログへのリンクも追加しました。 flatt.tech/cve/CVE-2021-2…	2021-10-29 05:54:22
@flatt_security	【2021年の注目記事を振り返る】 第3弾はMediumにおいて英語で公開したCVE-2021–20226の解説記事です！Hacker NewsやRedditで話題となり公開3日間で12,000PVを集めました。 flattsecurity.medium.com/cve-2021-20226…	2021-12-21 10:00:00
/r/ReverseEngineering	CVE-2021-20226: A reference-counting bug in the Linux kernel io_uring subsystem that can be leveraged for local privilege escalation	2021-04-22 16:49:14
/r/netsec	CVE-2021–20226 a reference counting bug which leads to local privilege escalation in io_uring.	2021-06-21 15:01:53
/r/RedSec	CVE-2021–20226 a reference counting bug which leads to local privilege escalation in io_uring.	2021-06-21

18:38:52

← Previous ID

Next ID→

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