



CVE-2022-1043

Published on: Not Yet Published

Last Modified on: 02/02/2023 05:13:00 PM UTC

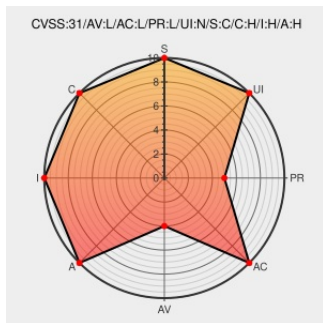
CVE-2022-1043

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 kernel's io_uring implementation. This flaw allows an attacker with a local account to corrupt system memory, crash the system or escalate privileges.

CVE-2022-1043 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVE References

Description	Tags	Link
io_uring: fix xa_alloc_cycle() error return value check · torvalds/linux@a30f895 · GitHub	github.com text/html	MISC github.com/torvalds/linux/commit/a30f895ad3239f45012e860d4f94c1a388b36d14
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2022-1043
io_uring Same Type Object Reuse Privilege Escalation ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/170834/io_uring-Same-Type-Object-Reuse-Privilege-Escalation.html
1997328 – (CVE-2022-1043) CVE-2022-1043 kernel: Linux Kernel io_uring I Use-After-Free Privilege	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1997328

comment@cve.report

179156 Debian Security Update for linux (CVE-2022-1043)

904101 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10796-1)

905809 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10796-2)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.14	rc1	All	All
Operating System	Linux	Linux Kernel	5.14	rc2	All	All
Operating System	Linux	Linux Kernel	5.14	rc3	All	All
Operating System	Linux	Linux Kernel	5.14	rc4	All	All
Operating System	Linux	Linux Kernel	5.14	rc5	All	All
Operating System	Linux	Linux Kernel	5.14	rc6	All	All
cpe:2.3:o:linux:linux_kernel:*.***:***:*						
cpe:2.3:o:linux:linux_kernel:5.14:rc1:*.***:***:*						
cpe:2.3:o:linux:linux_kernel:5.14:rc2:*.***:***:*						
cpe:2.3:o:linux:linux_kernel:5.14:rc3:*.***:***:*						
cpe:2.3:o:linux:linux_kernel:5.14:rc4:*.***:***:*						
cpe:2.3:o:linux:linux_kernel:5.14:rc5:*.***:***:*						
cpe:2.3:o:linux:linux_kernel:5.14:rc6:*.***:***:*						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-1043 : A flaw was found in the #Linux #kernel's io_uring implementation. This flaw allows an attacker with... twitter.com/i/web/status/1...	2022-08-29 15:12:42
 /r/netcve	CVE-2022-1043	2022-08-29 16:38:40
← 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](#)