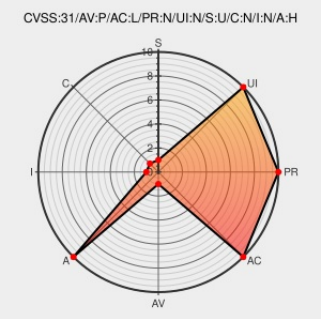
CVE-2023-4010

Published on: Not Yet Published

Last Modified on: 08/04/2023 05:06:00 PM UTC

CVE-2023-4010

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 USB Host Controller Driver framework in the Linux kernel. The usb_giveback_urb function has a logic loophole in its implementation. Due to the inappropriate judgment condition of the goto statement, the function cannot return under the input of a specific malformed descriptor file, so it falls into an endless loop, resulting in a denial of service.

CVE-2023-4010 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link
cve-details	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2023-4010
GitHub - wanrenmi/a-usb-kernel-bug: linux内核中的usb_giveback_urb函数在实现时存在逻辑漏洞，由于goto语句的判断条件不恰当，导致在特定的畸形描述符文件输入下该函数无法返回，陷入在死循环中占用CPU资源，导致拒绝服务攻击	github.com text/html	MISC github.com/wanrenmi/a-usb-kernel-bug
2227726 – (CVE-2023-4010) CVE-2023-4010 kernel: usb: hcd: malformed USB descriptor leads to infinite loop in usb_giveback_urb()	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=2227726

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

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	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All

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

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

cpe:2.3:o:redhat:enterprise_linux:9.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→