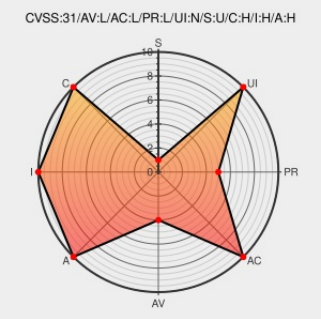
CVE-2023-3640

Published on: Not Yet Published

Last Modified on: 08/02/2023 01:49:00 PM UTC

CVE-2023-3640

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



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

A possible unauthorized memory access flaw was found in the Linux kernel's cpu_entry_area mapping of X86 CPU data to memory, where a user may guess the location of exception stacks or other important data. Based on the previous CVE-2023-0597, the 'Randomize per-cpu entry area' feature was implemented in /arch/x86/mm/cpu_entry_area.c, which works through the init_cea_offsets() function when KASLR is enabled. However, despite this feature, there is still a risk of per-cpu entry area leaks. This issue could allow a local user to gain access to some important data with memory in an expected location and potentially escalate their privileges on the system.

CVE-2023-3640 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

CVE References

Description	Tags	Link
2217523 – (CVE-2023-3640) CVE-2023-3640 Kernel: x86/mm: a per-cpu entry area leak was identified through the init_cea_offsets function when prefetchnta and prefetcht2 instructions being used for the per-cpu entry area mapping to the user space	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=2217523
cve-details	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2023-3640

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→