



CVE-2022-4543

Published on: Not Yet Published

Last Modified on: 02/12/2023 10:10:53 PM UTC

CVE-2022-4543

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

A flaw named "EntryBleed" was found in the Linux Kernel Page Table Isolation (KPTI). This issue could allow a local attacker to leak KASLR base via prefetch side-channels based on TLB timing for Intel systems.

CVE-2022-4543 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

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

CVE References

Description	Tags	Link
oss-security - CVE-2022-4543: KASLR Leakage Achievable even with KPTI through Prefetch Side-Channel	www.openwall.com text/x-c	MISC www.openwall.com/lists/oss-security/2022/12/16/3
Will's Root: EntryBleed: Breaking KASLR under KPTI with Prefetch (CVE-2022-4543)	www.willroot.io text/html	MISC www.willroot.io/2022/12/entrybleed.html

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.

Related QID Numbers

905246 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (12981)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @oss_security	CVE-2022-4543: KASLR Leakage Achievable even with KPTI through Prefetch Side-Channel: Posted by Will on Dec 16I've... twitter.com/i/web/status/1...	2022-12-16 22:42:02
 @linkersec	EntryBleed: Breaking KASLR under KPTI with Prefetch (CVE-2022-4543) An article about using Meltdown to bypass KASL... twitter.com/i/web/status/1...	2022-12-17 16:04:45
 @ipssignatures	The vuln CVE-2022-4543 has a tweet created 0 days ago and retweeted 10 times. twitter.com/linkersec/stat... #pow1rtrtwwcve	2022-12-17 22:06:01
 @Komodosec	#security #linux EntryBleed: Breaking KASLR under KPTI with Prefetch (CVE-2022-4543) willsroot.io/2022/12/entryb...	2022-12-17 23:14:33
 @Sujeet	CVE-2022-4543, named "EntryBleed" by Will from @cor_ctf; appears to have the potential to bypass KASLR on systems w... twitter.com/i/web/status/1...	2022-12-18 14:30:18
 @masami256	Will's Root: EntryBleed: Breaking KASLR under KPTI with Prefetch (CVE-2022-4543) willsroot.io/2022/12/entryb...	2022-12-18 23:33:52
 @ksg93rd	#Threat_Research EntryBleed: Breaking KASLR under KPTI with Prefetch (CVE-2022-4543) willsroot.io/2022/12/entryb...]-> seclists.org/oss-sec/2022/q...	2022-12-19 05:02:47
 @PentestingN	EntryBleed: Breaking KASLR under KPTI with Prefetch (CVE-2022-4543) Recently, I've discovered that Linux KPTI has i... twitter.com/i/web/status/1...	2022-12-19 07:14:46
 @SeYasashi	メルトダウンとかスペクターに関係するintel製cpuの脆弱性ぽいな access.redhat.com/security/cve/c...	2022-12-19 11:22:36
 @_bcoles	Support for #EntryBleed prefetch #KASLR bypass (CVE-2022-4543) added to KASLD - github.com/bcoles/kasld Should wor... twitter.com/i/web/status/1...	2022-12-21 15:14:48
 @kmkz_security	EntryBleed: Breaking KASLR under KPTI with Prefetch (CVE-2022-4543) willsroot.io/2022/12/entryb...	2022-12-21 20:41:00
 @ipssignatures	The vuln CVE-2022-4543 has a tweet created 0 days ago and retweeted 10 times. twitter.com/kmkz_security/... #pow1rtrtwwcve	2022-12-22 12:06:00
 @ipssignatures	The vuln CVE-2022-4543 has a tweet created 1 days ago and retweeted 10 times. twitter.com/_bcoles/status... #pow1rtrtwwcve	2022-12-23 08:06:01
 @Dinosn	EntryBleed: Breaking KASLR under KPTI with Prefetch (CVE-2022-4543) reddit.com/r/lowlevel/com...	2022-12-23 18:55:41
 @CVEreport	CVE-2022-4543 : A flaw named "EntryBleed" was found in the #Linux Kernel Page Table Isolation KPTI . This issue co... twitter.com/i/web/status/1...	2023-01-11 15:04:48
 /r/linkersec	EntryBleed: Breaking KASLR under KPTI with Prefetch (CVE-2022-4543)	2022-12-17 16:05:22

		18:05:33
 /r/lowlevel	EntryBleed: Breaking KASLR under KPTI with Prefetch (CVE-2022-4543)	2022-12-22 07:44:00
 /r/netcve	CVE-2022-4543	2023-01-11 15:40:16
 /r/CyberExploits	CVE-2022-4543 Linux Kernel Page Table Isolation EntryBleed information disclosure	2023-01-11 18:25:33
← 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](#)