



CVE-2017-14954

Published on: 09/30/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:45 PM UTC

CVE-2017-14954

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

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

The waitid implementation in kernel/exit.c in the Linux kernel through 4.13.4 accesses rusage data structures in unintended cases, which allows local users to obtain sensitive information, and bypass the KASLR protection mechanism, via a crafted system call.

CVE-2017-14954 has been assigned by [M](#) cve@mitre.org 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

CVSS2 Score: **2.1 - LOW**

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

CVE References

Description	Tags	Link
kernel/git/torvalds/linux.git - Linux kernel source tree	Issue Tracking Patch Third Party Advisory git.kernel.org text/html	MISC git.kernel.org/cgiit/linux/kernel/git/torvalds/linux.git/commit/?id=6c85501f2fabcf4fc6ed976543d252c4eaf4be9

argp na Twitterze: "Linux kernel 4.13 waitid(2) 144 bytes infoleak by spender: https://t.co/0yzDYK6uLM"

Third Party Advisory

nitter.domain.glass

text/html

MISC twitter.com/_argp/status/914021130712870912

grsecurity na Twitterze: "The infoleak was neither inserted nor discovered by me, just the exploit (couple minutes of work, no big deal)... "

Third Party Advisory

nitter.domain.glass

text/html

MISC twitter.com/grsecurity/status/914079864478666753

Third Party Advisory

grsecurity.net

text/x-c

MISC grsecurity.net/~spender/exploits/wait_for_kaslr_to_be_effective.c

fix infoleak in waitid(2) · torvalds/linux@6c85501 · GitHub

Issue Tracking

Patch

Third Party Advisory

github.com

text/html

MISC

github.com/torvalds/linux/commit/6c85501f2fabcf4c6ed976543d252c4eaf4be9

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

No vendor comments have been submitted for this CVE

← 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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/mitre).

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