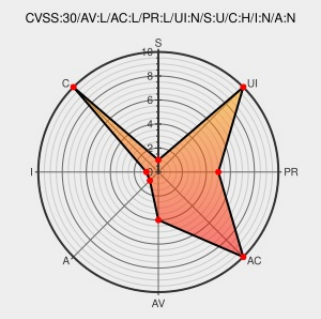
CVE-2017-14954

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 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/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=6c85501f2fabcfc4fc6ed976543d252c4eaf4be9

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/6c85501f2fabcfc4fc6ed976543d252c4eaf4be9

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→