

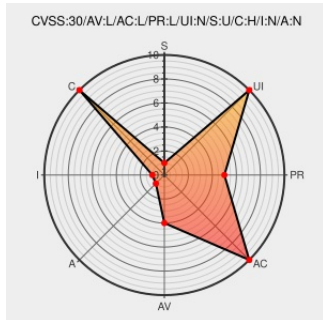


CVE-2017-15537

Published on: 10/17/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:33 PM UTC

CVE-2017-15537

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

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

The x86/fpu (Floating Point Unit) subsystem in the Linux kernel before 4.13.5, when a processor supports the xsave feature but not the xsaves feature, does not correctly handle attempts to set reserved bits in the xstate header via the ptrace() or rt_sigreturn() system call, allowing local users to read the FPU registers of other processes on the system, related to arch/x86/kernel/fpu/regset.c and arch/x86/kernel/fpu/signal.c.

CVE-2017-15537 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	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=814fb7bb7db5433757d76f4c4502c96fc53b0b5e

Third Party Advisory

git.kernel.org

text/html

x86/fpu: Don't let userspace set bogus xcomp_bv · torvalds/linux@814fb7b · GitHub

Issue Tracking

Patch

Third Party Advisory

github.com

text/html

CONFIRM

github.com/torvalds/linux/commit/814fb7bb7db5433757d76f4c4502c96fc53b0b5e

Release Notes

Vendor Advisory

www.kernel.org

text/plain

CONFIRM

www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.13.5

Pixel/Nexus Security Bulletin—January 2018 | Android Open Source Project

source.android.com

text/html

CONFIRM

source.android.com/security/bulletin/pixel/2018-01-01

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](#) 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](#)