

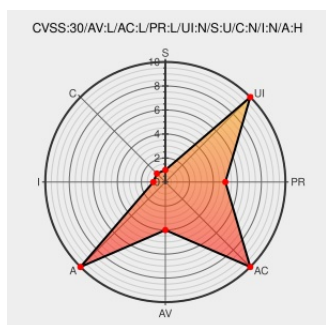


CVE-2018-1091

Published on: 03/27/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:32 PM UTC

CVE-2018-1091

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

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

In the `flush_tmregs_to_thread` function in `arch/powerpc/kernel/ptrace.c` in the Linux kernel before 4.13.5, a guest kernel crash can be triggered from unprivileged userspace during a core dump on a POWER host due to a missing processor feature check and an erroneous use of transactional memory (TM) instructions in the core dump path, leading

to a denial of service.

CVE-2018-1091 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	NONE	NONE	HIGH

CVSS2 Score: **4.9 - MEDIUM**

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

CVE References

Description	Tags	Link
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory	CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=c1fa0768a8713b135848f78fd43ffc208d8ded70

	git.kernel.org text/html	
1558149 – (CVE-2018-1091) CVE-2018-1091 kernel: guest kernel crash during core dump on POWER9 host	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1558149
'[PATCH v2] powerpc/tm: Flush TM only if CPU has TM feature' - MARC	Patch Third Party Advisory marc.info text/x-diff	CONFIRM marc.info/?l=linuxppc-embedded&m=150535531910494&w=2
oss-security - CVE-2018-1091: Linux kernel: a KVM guest kernel crash during core dump on POWER9 host	Mailing List Third Party Advisory openwall.com text/html	CONFIRM openwall.com/lists/oss-security/2018/03/27/4
powerpc/tm: Flush TM only if CPU has TM feature · torvalds/linux@c1fa076 · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/c1fa0768a8713b135848f78fd43ffc208d8ded70
CVE-2018-1091 - Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	CONFIRM access.redhat.com/security/cve/cve-2018-1091
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2018:1318
	Patch Vendor Advisory www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.13.5

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 →](#)

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](#)