



CVE-2018-18021

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2018-18021
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-07 06:29:00 UTC
Updated	2019-04-03 01:29:00 UTC
Description	arch/arm64/kvm/guest.c in KVM in the Linux kernel before 4.18.12 on the arm64 platform mishandles the KVM_SET_ON_F

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link
cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.18.12	MISC	cdn.kernel.org
Debian -- Security Information -- DSA-4313-1 linux	DEBIAN	www.debian.org
oss-security - arm64 Linux kernel: Privilege escalation by taking control of the KVM hypervisor	MISC	www.openwall.com
arm64: KVM: Sanitize PSTATE.M when being set from userspace · torvalds/linux@2a3f934 · GitHub	MISC	github.com
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
USN-3821-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com

USN-3931-1: Linux kernel vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
USN-3931-2: Linux kernel (HWE) vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
arm64: KVM: Tighten guest core register access from userspace · torvalds/linux@d26c25a · GitHub	MISC	github.com
USN-3821-2: Linux kernel (Xenial HWE) vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com
Linux Kernel 'arch/arm64/kvm/guest.c' Local Privilege Escalation Vulnerability	BID	www.securityfocus.com
Red Hat Customer Portal	REDHAT	access.redhat.com
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.