CVE-2017-12188

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-12188
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-11 15:29:00 UTC
Updated	2024-04-02 18:05:00 UTC
Description	arch/x86/kvm/mmu.c in the Linux kernel through 4.13.5, when nested virtualisation is used, does not properly traverse gues

Risk And Classification

Problem Types: CWE-121

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link
[2/2] KVM: MMU: always terminate page walks at level 1 - Patchwork	CONFIRM	patchwo
[1/2] KVM: nVMX: update last_nonleaf_level when initializing nested EPT - Patchwork	CONFIRM	patchwo
CVE-2017-12188 - Red Hat Customer Portal	MISC	access.r
1500380 – (CVE-2017-12188) CVE-2017-12188 Kernel: KVM: MMU potential stack buffer overrun during page walks	CONFIRM	bugzilla.r
Red Hat Customer Portal	REDHAT	access.r
Linux Kernel CVE-2017-12188 Remote Buffer Overflow Vulnerability	BID	www.sec
Red Hat Customer Portal	REDHAT	access.r
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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