



CVE-2018-12904

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

Summary

CVE	CVE-2018-12904
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-27 11:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	In arch/x86/kvm/vmx.c in the Linux kernel before 4.17.2, when nested virtualization is used, local attackers could cause L1

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	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	Tags
USN-3752-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	Third Party
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	Patch
USN-3752-2: Linux kernel (HWE) vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	Third Party
KVM (Nested Virtualization) - L1 Guest Privilege Escalation - Linux dos Exploit	EXPLOIT-DB	www.exploit-db.com	Exploit
kvm: nVMX: Enforce cpl=0 for VMX instructions · torvalds/linux@727ba74 · GitHub	MISC	github.com	Patch
cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.17.2	MISC	cdn.kernel.org	Release
1589 - project-zero - Project Zero - Monorail	MISC	bugs.chromium.org	Exploit
USN-3752-3: Linux kernel (Azure, GCP, OEM) vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	Third Party

CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc
No vendor comments have been submitted for this CVE.			
There are currently no legacy QID mappings associated with this CVE.			

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API cve.report/api

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