CVE-2017-16994

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

Summary

CVE	CVE-2017-16994
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-27 19:29:00 UTC
Updated	2018-04-25 01:29:00 UTC
Description	The walk_hugetlb_range function in mm/pagewalk.c in the Linux kernel before 4.14.2 mishandles holes in hugetlb ranges, v

Risk And Classification

Problem Types: CWE-200

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	Tags
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org	Patch
USN-3619-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	
mm/pagewalk.c: report holes in hugetlb ranges · torvalds/linux@373c455 · GitHub	CONFIRM	github.com	Patch
USN-3617-2: Linux (HWE) vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	
Linux Kernel - 'mincore()' Uninitialized Kernel Heap Page Disclosure - Linux dos Exploit	EXPLOIT-DB	www.exploit-db.com	Exploit,
USN-3619-2: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	
1431 - Linux: mincore() discloses uninitialized kernel heap pages - project-zero - Monorail	CONFIRM	bugs.chromium.org	Exploit,
USN-3617-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	
Linux Kernel 'mm/pagewalk.c' Local Information Disclosure Vulnerability	BID	www.securityfocus.com	Third P
USN-3617-3: Linux kernel (Raspberry Pi 2) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	
Red Hat Customer Portal	REDHAT	access.redhat.com	
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.14.2	CONFIRM	www.kernel.org	Releas

USN-3632-1: Linux kernel (Azure) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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