CVE-2017-16995

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

Summary

CVE	CVE-2017-16995
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-27 17:08:00 UTC
Updated	2023-01-19 15:48:00 UTC
Description	The check_alu_op function in kernel/bpf/verifier.c in the Linux kernel through 4.4 allows local users to cause a denial of ser

Risk And Classification

Problem Types: CWE-119

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	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	Tags
Linux Kernel CVE-2017-16995 Local Memory Corruption Vulnerability	BID	www.securityfocus.com	Third P
USN-3633-1: Linux kernel (Intel Euclid) vulnerability | Ubuntu security notices	UBUNTU	usn.ubuntu.com	
bpf: fix incorrect sign extension in check_alu_op() · torvalds/linux@95a762e · GitHub	MISC	github.com	Third P
USN-3619-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	
USN-3619-2: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	
1454 - arbitrary read+write via incorrect range tracking in eBPF - project-zero - Monorail	MISC	bugs.chromium.org	Third P
Linux - BPF Sign Extension Local Privilege Escalation (Metasploit) - Linux local Exploit	EXPLOIT-DB	www.exploit-db.com	
Debian -- Security Information -- DSA-4073-1 linux	DEBIAN	www.debian.org	Third P

Linux Kernel < 4.13.9 (Ubuntu 16.04/Fedora 27) - Local Privilege Escalation	EXPLOIT-DB	www.exploit-db.com	
Exploit – Page 44298 – Exploits Database	EXPLOIT-DB	www.exploit-db.com	
USN-3523-2: Linux kernel (HWE) vulnerabilities | Ubuntu	UBUNTU	usn.ubuntu.com	
kernel/git/tip/tip.git - Unnamed repository; edit this file 'description' to name the repository.	CONFIRM	git.kernel.org	
oss-security - Linux >=4.9: eBPF memory corruption bugs	MISC	openwall.com	Mailing
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	Vendor
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.

Free CVE JSON API cve.report/api

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