



CVE-2018-18445

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

Summary

CVE	CVE-2018-18445
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-17 19:29:00 UTC
Updated	2023-01-17 21:34:00 UTC
Description	In the Linux kernel 4.14.x, 4.15.x, 4.16.x, 4.17.x, and 4.18.x before 4.18.13, faulty computation of numeric bounds in the BP

Risk And Classification

Problem Types: CWE-125

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	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	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	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.6	All	All	All

Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References				
Reference	Source	Link	Tags	
USN-3847-3: Linux kernel (Azure) vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	Threat Intelligence	
USN-3832-1: Linux kernel (AWS) vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	Threat Intelligence	
USN-3835-1: Linux kernel vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	Threat Intelligence	
Red Hat Customer Portal	REDHAT	access.redhat.com	Threat Intelligence	
bpf: 32-bit RSH verification must truncate input before the ALU op · torvalds/linux@b799207 · GitHub	MISC	github.com	Patch	
Red Hat Customer Portal	REDHAT	access.redhat.com	Threat Intelligence	
cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.18.13	MISC	cdn.kernel.org	Patch	
USN-3847-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	Threat Intelligence	
support.f5.com/csp/article/K38456756	CONFIRM	support.f5.com		
1686 - project-zero - Project Zero - Monorail	MISC	bugs.chromium.org	Issue	
USN-3847-2: Linux kernel (HWE) vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	Threat Intelligence	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	Patch	
cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.14.75	MISC	cdn.kernel.org	Patch	
CVE Program record	CVE.ORG	www.cve.org	Canonical	
NVD vulnerability detail	NVD	nvd.nist.gov	Canonical	

No vendor comments have been submitted for this CVE.

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

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