CVE-2019-11190

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

Summary

CVE	CVE-2019-11190
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-12 00:29:00 UTC
Updated	2019-06-07 07:29:00 UTC
Description	The Linux kernel before 4.8 allows local users to bypass ASLR on setuid programs (such as /bin/su) because install_exec_

Risk And Classification

Problem Types: CWE-362

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
[SECURITY] [DLA 1799-2] linux security update	MLIST	lists.debian.org	
[security-announce] openSUSE-SU-2019:1570-1: important: Security update	SUSE	lists.opensuse.org	
[SECURITY] [DLA 1799-1] linux security update	MLIST	lists.debian.org	
USN-4008-2: AppArmor update | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	
USN-4008-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	
www.openwall.com/lists/oss-security/2019/04/03/4/1	MISC	www.openwall.com	Exploit, Mailing List
oss-security - Re: Linux kernel < 4.8 local generic ASLR - CVE-ID	MLIST	www.openwall.com	
Linux Kernel CVE-2019-11190 Local Security Bypass Vulnerability	BID	www.securityfocus.com	
kernel/git/stable/stable-queue.git - Linux kernel stable patch queue	MISC	git.kernel.org	Patch, Third Party A
kernel/git/stable/stable-queue.git - Linux kernel stable patch queue	MISC	git.kernel.org	Patch, Third Party A
USN-4008-3: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	
oss-security - Linux kernel < 4.8 local generic ASLR bypass for setuid binaries	MISC	www.openwall.com	Exploit, Mailing List

CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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