CVE-2018-18955

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

Summary

CVE	CVE-2018-18955
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-11-16 20:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	In the Linux kernel 4.15.x through 4.19.x before 4.19.2, map_write() in kernel/user_namespace.c allows privilege escalation

Risk And Classification

Problem Types: CWE-863

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	18.10	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

References

Reference	Source	Link
1712 - Linux: broken uid/gid mapping for nested user namespaces with >5 ranges - project-zero - Monorail	MISC	bugs.chromium.
USN-3832-1: Linux kernel (AWS) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
support.f5.com/csp/article/K39103040	CONFIRM	support.f5.com
USN-3835-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
Linux - Nested User Namespace idmap Limit Local Privilege Escalation (Metasploit) - Linux local Exploit	EXPLOIT-DB	www.exploit-db.

cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.18.19	MISC	cdn.kernel.org
CVE-2018-18955 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.c
cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.2	MISC	cdn.kernel.org
userns: also map extents in the reverse map to kernel IDs · torvalds/linux@d2f007d · GitHub	MISC	github.com
USN-3836-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
Linux - Broken uid/gid Mapping for Nested User Namespaces - Linux local Exploit	EXPLOIT-DB	www.exploit-db.c
USN-3836-2: Linux kernel (HWE) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
USN-3833-1: Linux kernel (AWS) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
Linux Kernel CVE-2018-18955 Local Privilege Escalation Vulnerability	BID	www.securityfoc
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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**