CVE-2017-7184

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

Summary

CVE	CVE-2017-7184
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-19 18:59:00 UTC
Updated	2023-02-10 00:53:00 UTC
Description	The xfrm_replay_verify_len function in net/xfrm/xfrm_user.c in the Linux kernel through 4.10.6 does not validate certain size

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.10	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	4.8	All	All	All
Operating System	Linux	Linux Kernel	4.8	All	All	All

References

Reference
Android Security Bulletin—May 2017 | Android Open Source Project
Red Hat Customer Portal
kernel/git/torvalds/linux.git - Linux kernel source tree
The Results – Pwn2Own 2017 Day One -
Red Hat Customer Portal
Ubuntu Linux Falls on Day 1 of Pwn2Own Hacking Competition | eWEEK
Red Hat Customer Portal
Zero Day Initiative on Twitter: "Chaitin Security Research Lab (@ChaitinTech) welcomes Ubuntu to #Pwn2Own with a Linux kernel heap OOB
kernel/git/torvalds/linux.git - Linux kernel source tree

Linux Kernel CVE-2017-7184 Local Privilege Escalation Vulnerability
xfrm_user: validate XFRM_MSG_NEWAE incoming ESN size harder · torvalds/linux@f843ee6 · GitHub
oss-security - CVE-2017-7184: kernel: Local privilege escalation in XFRM framework
Red Hat Customer Portal
xfrm_user: validate XFRM_MSG_NEWAE XFRMA_REPLAY_ESN_VAL replay_window · torvalds/linux@677e806 · GitHub
Linux Kernel Out-of-Bounds Memory Error in XFRM xfrm_replay_verify_len() Lets Local Users Gain Elevated Privileges - SecurityTracker
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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