CVE-2014-8709

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

Summary

CVE	CVE-2014-8709
State	PUBLIC
Assigner	security@microfocus.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-10 11:55:00 UTC
Updated	2023-11-07 02:22:00 UTC
Description	The ieee80211_fragment function in net/mac80211/tx.c in the Linux kernel before 3.13.5 does not properly maintain a certa

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	3.13	All	All	All
Operating System	Linux	Linux Kernel	3.13.1	All	All	All
Operating System	Linux	Linux Kernel	3.13.2	All	All	All
Operating System	Linux	Linux Kernel	3.13.3	All	All	All
Operating System	Linux	Linux Kernel	3.13	All	All	All
Operating System	Linux	Linux Kernel	3.13.1	All	All	All
Operating System	Linux	Linux Kernel	3.13.2	All	All	All
Operating System	Linux	Linux Kernel	3.13.3	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference
Red Hat Customer Portal
mac80211: fix fragmentation code, particularly for encryption · torvalds/linux@338f977 · GitHub
Linux Kernel 'net/mac80211/tx.c' Information Disclosure Vulnerability
Android Security Bulletin—March 2017 | Android Open Source Project
[security-announce] SUSE-SU-2015:0652-1: important: Security update for

Android Multiple Flaws Let Users Deny Service, Obtain Potentially Sensitive Information, and Gain Elevated Privileges and Let Remote Users
kernel/git/torvalds/linux.git - Linux kernel source tree
oss-security - Re: CVE Request: Linux kernel mac80211 plain text leak
[security-announce] openSUSE-SU-2015:0566-1: important: kernel update fo
www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.13.5
IBM X-Force Exchange
[security-announce] SUSE-SU-2015:0481-1: important: Security update for
kernel/git/torvalds/linux.git - Linux kernel source tree
Red Hat Customer Portal
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.