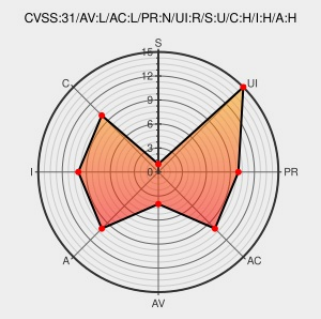
CVE-2015-0571

Published on: 05/09/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:18 PM UTC

CVE-2015-0571

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Linux Kernel from Linux contain the following vulnerability:

The WLAN (aka Wi-Fi) driver for the Linux kernel 3.x and 4.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not verify authorization for private SET IOCTL calls, which allows attackers to gain privileges via a crafted application, related to wlan_hdd_hostapd.c and wlan_hdd_wext.c.

CVE-2015-0571 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Android Security Bulletin—May 2016 | Android Open Source Project	Vendor Advisory, source.android.com, text/html	CONFIRM source.android.com/security/bulletin/2016-05-01.html

RETIRED: Huawei Smart Phones Memory Buffer Overflow Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 77691
Multiple Issues in WLAN Driver Allow Local Privilege Escalation (CVE-2015-0569, CVE-2015-0570, CVE-2015-0571) | Code Aurora	Broken Link web.archive.org text/html Inactive Link Not Archived	CONFIRM www.codeaurora.org/projects/security-advisories/multiple-issues-wlan-driver-allow-local-privilege-escalation-cve-2015

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→