CVE-2020-11832/CVE-2020-11833/CVE-2020-11834/CVE-2020-11835 Charger Modules Vulnerabilities

2020-11-30

OPPO security team sincerely appreciates these security researchers' efforts to help us improve the security level of OPPO products. And we encourage more security researchers to apply for CVE IDs.

Acknowledgements

Vulnerabilities Submitted by: Li Qingyu, Li Ke, Chen Wu, Lu Xianfeng

Vulnerabilities Severity:Medium

Submission Date:Nov.10th, 2020

1. CVE-2020-11832

The out of bounds write access vulnerabilities are found in charging_limit_current_write/charging_limit_time_write/#chg_log_write/critical_log_write/ functions

[PRODUCT/VERSION]:

For charging_limit_current_write/# charging_limit_time_write/#critical_log_write/ functions:

Model: 19362_user_debug

Kernel: Linux localhost 4.19.110-perf+ #1 SMP PREEMPT Sat Sep 26 11:37:36 CST 2020 aarch64

fingerprint:

[ro.build.fingerprint]: [OPPO/CPH2025EEA/OP4BA2L1:11/RKQ1.200809.001/1601091005879:user/release-keys]]

For chg_log_write function:

[PRODUCT/VERSION]:

Model: 19551_user_debug

Kernel: Linux version 4.19.127-06551-g661a4be629e1-dirty (nobody@android-build) (Android (6443078 based on r383902)

clang version 11.0.1

(https://android.googlesource.com/toolchain/llvm-

projectb397f81060ce6d701042b782172ed13bee898b79),LLD11.0.1(/buildbot/tmp/tmp6_m7QHb397f81060ce6d701042b782172ed13bee898b79)) #1 SMP

PREEMPT Wed Sep 30 07:48

fingerprint:

[ro.build.fingerprint]: [OPPO/CPH2035/OP4C5FL1:11/RP1A.200709.001/1601423719080:user/release-keys]

[PROBLEM TYPE]:DOS Overflow

[DESCRIPTION]:

Many functions in /SM8250_Q_Master/android/vendor/oppo_charger/oppo/oppo_charger.c have not checked the parameters

2. CVE-2020-11833

The out of bounds write access vulnerability is found in mp2650_data_log_write function.

[PRODUCT/VERSION]:Model: 19362_user_debug

Kernel: Linux localhost 4.19.110-perf+ #1 SMP PREEMPT Sat Sep 26 11:37:36 CST 2020 aarch64

fingerprint:

[ro.build.fingerprint]: [OPPO/CPH2025EEA/OP4BA2L1:11/RKQ1.200809.001/1601091005879:user/release-keys]]

[PROBLEM TYPE]:DOS Overflow

[DESCRIPTION]:

In /SM8250_Q_Master/android/vendor/oppo_charger/oppo/charger_ic/oppo_mp2650.c

The function mp2650_data_log_write in mp2650_data_log_write does not check the parameter len which causes a vulnerability.

3. CVE-2020-11834

The out of bounds write access vulnerability is found in proc_fastchg_fw_update_write function.

[PRODUCT/VERSION]Model: 19362_user_debug

Kernel: Linux localhost 4.19.110-perf+ #1 SMP PREEMPT Sat Sep 26 11:37:36 CST 2020 aarch64

fingerprint:

[ro.build.fingerprint]: [OPPO/CPH2025EEA/OP4BA2L1:11/RKQ1.200809.001/1601091005879:user/release-keys]]

[PROBLEM TYPE]:DOS Overflow

[DESCRIPTION]:

In /SM8250_Q_Master/android/vendor/oppo_charger/oppo/oppo_vooc.c

The function proc_fastchg_fw_update_write in proc_fastchg_fw_update_write does not check the parameter len, resulting in a vulnerability.

4.CVE-2020-11835

The out of bounds write access vulnerability is found in proc_work_mode_write function.

[PRODUCT/VERSION]:Model: 19362_user_debug

Kernel: Linux localhost 4.19.110-perf+ #1 SMP PREEMPT Sat Sep 26 11:37:36 CST 2020 aarch64

fingerprint:

[ro.build.fingerprint]: [OPPO/CPH2025EEA/OP4BA2L1:11/RKQ1.200809.001/1601091005879:user/release-keys]]

[PROBLEM TYPE]:DOS

[DESCRIPTION]:

In /SM8250_Q_Master/android/vendor/oppo_charger/oppo/charger_ic/oppo_da9313.c

Failure to check the parameter buf in the function proc_work_mode_write in proc_work_mode_write causes a vulnerability.

CVE Link :

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11832

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11833

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11834

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11835