



[Notice](#) > Notice details

## 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>

[OPPO Official Website](#)

[ColorOS](#)

[Submit Vulnerability Report](#)

[Privacy Policy](#)

[Get PGP Public Key](#)

[Functional Email](#)

[Twitter](#)

[Facebook](#)