

Forum:[Hack Forums](#)

Thread: [\[2025\] ? List of all Android devices LE can crack with Cellebrite ?](#)

Bastille - April 21, 2025, 11:18 am

(if you don't read the entire thread, please at least check the end, thanks)

Access to smartphones by authorities is a recurring concern for data privacy. It has been discussed a few times on the forum, notably through the tool/device from the company Cellebrite : <https://cellebrite.com>

This topic is very interesting, and the vulnerabilities now rely more on hardware instead of software (Android - keeping your smartphone up to date do not protect you anymore).

The information has been revealed by Osservatorio Nessuno which is a non-profit org related to data privacy (and also participate to the Tor project). The matrix provided by Cellebrite are not intended to be shared, but times to times they leak : <https://osservatorionessuno.org/blog/2025/03/a-deep-dive-into-cellebrite-android-support-as-of-february-2025/>

Quote:Cellebrite, as far as we know, publishes a support matrix for Android-based and iOS-based devices monthly or at least multiple times a year. The latest version available at time of writing is version 7.73.1 released on February 2025.

For [Capabilities] there are two methods, with 2 level of success : green (you're cooked) and yellow (you're not necessarily cooked, for the time being) : ? Full extraction of data even when turned off, or turned on without being unlocked once since the boot.

? Brute-force password

? Partial extraction of data even when turned off, or turned on without being unlocked once since the boot.

? Brute-force password work partially

Samsung (Android 7 to 14, potentially 15) (Exynos / MTK / Qualcomm chipset based)

Capabilities : ? Full extraction of data even when turned off, or turned on without being unlocked once since the boot.

? Brute-force password

Code • Galaxy S7 / S7 Edge
• Galaxy S8 / S8+

- Galaxy S9 / S9+
 - Galaxy S10e / S10 / S10+ / S10 Lite
 - Galaxy S20 / S20+ / S20 Ultra / S20 FE (4G and 5G)
 - Galaxy S21 / S21+ / S21 Ultra / S21 FE
 - Galaxy S22 / S22+ / S22 Ultra
 - Galaxy S23 / S23+ / S23 Ultra
 - Galaxy S24 / S24+ / S24 Ultra (Snapdragon 8 Gen 3 / Exynos 2400)
 - Galaxy Note 8 / 9 / 10 / 10+ / 10 Lite / 20 / 20 Ultra
 - Galaxy A50 / A51 / A52 / A52s / A53 / A54
 - Galaxy A13 / A14 / A22 / A23 / A33 / A34 / A72
 - Galaxy A32 (4G Dimensity / 5G Dimensity)
 - Galaxy A12 / A20s / A21s / A03s / A05 / A05s
 - Galaxy M12 / M13 / M14 / M21 / M22 / M31 / M32 / M33 / M51 / M53 / M54
 - Galaxy F05 / F12 / F22 / F23 / F41 / F42 / F62 / F04 / F14 / F15
 - Galaxy Z Flip / Z Flip 3 / 4 / 5
 - Galaxy Z Fold / Fold 2 / 3 / 4 / 5
 - Galaxy XCover 4s / 5 / 6 Pro
 - Galaxy Tab A7 / A8 / S6 Lite / S7 / S8 / S9 series
 - Galaxy M05, M55s
- Huawei (Chipsets Kirin / MTK / Qualcomm[/color])

Capabilities : ? Full extraction of data even when turned off, or turned on without being unlocked once since the boot.

? Brute-force password : partially

Code • Huawei P10 / P20 / P30 / P40 / P50 / P60 / Pura 70

- Huawei Mate 9 / 10 / 20 / 30 / 40 / 50 / 60
- Huawei Mate X2 / X3 / Xs 2
- Huawei Nova / Nova 2 / 3 / 5T / 7 / 8 / 9 / 10 / 11 / 12
- Huawei Nova 8 SE / Nova Y60 / Y6s / Y6p / Y7a / Y9a
- Honor 10 / 20 / 8A / 9 Lite / Play 9A

Huawei, LG, Motorola, Xiaomi, Sony, OnePlus and others (Qualcomm chipset based)

Capabilities : ? Full extraction of data even when turned off, or turned on without being unlocked once since the boot.

? Brute-force password

Code • Huawei Nova / Nova 9 / Nova 10 / Nova 11

- Huawei P50 Pro
- Huawei Mate 50 Pro
- Honor 20 / 20 Pro
- LG G5 / G6 / G7 ThinQ / G8 ThinQ / G8X
- LG V30 / V40 / V50 ThinQ / V60 ThinQ
- LG Velvet
- LG Q6 / Q7 Alpha / Q7 Plus
- LG K40 / K92 5G
- Moto Z / Z2 Force / Z3 / Z4
- Moto X4
- Motorola Edge / Edge+ / Edge 20 / Edge 30

/ Edge 30 Pro / Edge 60 Ultra

- Moto G5 / G6 / G7 / G8 / G9 / G10 / G100

/ G Power / G Stylus

- Moto E4 / E5 / E6 / E7

- Xiaomi Mi 5 / Mi 6 / Mi 8 / Mi 9 / Mi 10 / Mi 11

/ 11 Lite 5G NE / 12 / 13 / 15

- Redmi Note 3 Pro / Note 5 / Note 6 Pro / Note 7 / Note 8 / Note 9S / Note 10 / Note 10 Pro

- Poco F1 / F2 Pro / F3

- Poco X3 / X4 Pro

- Xperia XZ / XZ1 / XZ2 / XZ3

- Xperia 1 / 1 II / 1 III / 1 IV / 1 V

- Xperia 5 / 5 II / 5 III / 5 IV

- Xperia 10 / 10 II / 10 III / 10 IV / 10 V

- OnePlus 3 / 3T / 5 / 5T / 6 / 6T / 7 / 7 Pro / 7T / 8 / 8 Pro / 9 / 9 Pro / 13

- OnePlus N-o-r-d / N-o-r-d CE / N-o-r-d CE 2 Lite

- Nokia 3 / 5 / 6 / 6.1 / 7 Plus / 7.1 / 7.2 / 8 / 8.1 / 8.3 5G / 9 PureView

- HTC U11 / U11 Life / U12+

- Asus ZenFone 3 Deluxe / ZenFone 4 / ZenFone 5 / ZenFone 6

- ROG Phone / ROG Phone II

- Oppo Find X2 Pro

- Oppo Reno 10x Zoom

- Realme GT / X2 / X3 / X50 Pro

- ZTE Axon 7 / 9 Pro / 10 Pro

Xiaomi, Huawei, LG, Motorola (MTK chipset based)

Capabilities : ? Full extraction of data even when turned off, or turned on without being unlocked once since the boot.

? Brute-force password

Code • Xiaomi 11T / 14T / 14T Pro

- Redmi Note 8 Pro / 9 / 9T / 10S / 11 / 11S / 11 Pro+ 5G / 13 5G / 13 Pro+ 5G

- Redmi A3 / A3 Pro

- Poco M3 Pro 5G / M4 Pro 5G / X3 GT

- Huawei Y5 (2019) / Y6p / Y6s / Nova 8 SE / Nova Y60

- Honor 8A / Play 9A (no recent models with MediaTek after 2022)

- LG Q7 (standard) / Stylo 3 / K7 / K8 / K12+ / K31 / W30 (no recent models after 2021 - production stopped)

- Moto E6s / E7 / G20 / G22 / G31 / G 2025 / G15 / G15 Power

Vivo, Oppo, Realme, OnePlus, Tecno, Infinix (MTK chipset based)

Capabilities : ? Partial extraction of data even when turned off, or turned on without being unlocked once since the boot.

? Brute-force password partially works

Code • Vivo V15 / V17 (Inde) / S1 / Y12s / Y19 / Y20 / Y53s / Y73

- Vivo V21 5G / V23 5G

- Vivo X70t / X80 / X90s

- Vivo S6 5G / S15e

- Vivo Y52 5G / Y73 / Y53s

- Vivo Y100 / Y100A (Helio G99)
 - Vivo X200 / X200S (Dimensity 9400 / 9400+)
 - Oppo F5 / F9 / A31 / A54 / A94
 - Oppo A96 (Helio G88)
 - Oppo Reno 2Z / 3 Pro (global) / 5 Z / 6 Z
 - Oppo Reno 6 5G / 7 5G / 8 5G / 8 Pro (China)
 - Oppo A78 (2023) – Dimensity 700
 - Realme 1 / 3 / 6 / 7 / 7 5G / 8 / 8 5G
 - Realme X7 / X7 Max / X7 Pro
 - Realme GT Neo / GT Neo3 (Dimensity 8100)
 - Realme Narzo 20 / 30 / 30 5G / 50 / 50A / 60x (Dimensity 6100+)
 - Realme C25s / C55 / C67 / Narzo N53
 - Realme Neo7 SE (Dimensity 8400)
 - OnePlus N-o-r-d 2 / N-o-r-d 2T / N-o-r-d CE 2 / N-o-r-d 3
 - OnePlus Ace / Ace 2V / Ace 5V / Ace 5S / Ace Racing Edition (Dimensity 8100 / 9000 / 9400 / 9350)
 - Tecno Camon 16 / 16 Premier / 18 / 18 Premier / 20 Premier (Dimensity 8050)
 - Tecno Spark 6 / 8
 - Tecno Pova 2
 - Tecno Phantom X / Phantom X2 (Dimensity 920)
 - Infinix Note 7 / 8 / 10 / 10 Pro / 11 / 11 Pro / 12 / 12 Pro
 - Infinix Zero 8 / Zero X Pro / Zero 20
 - Infinix Hot 10 / 11 / 12
- Motorola, Vivo, Meizu (Exynos chipset based)

Capabilities : ? Full extraction of data even when turned off, or turned on without being unlocked once since the boot.

? Brute-force password

Code • Motorola One Vision / One Action / One Vision (China = Motorola P50)

- Vivo X30 / X30 Pro – Exynos 980
- Vivo S6 5G – Exynos 980
- Vivo Y70s / Y51s – Exynos 880
- Vivo X60 / X60 Pro (China version only) – Exynos 1080
- Vivo S15e – Exynos 1080
- Meizu Pro 5 – Exynos 7420
- Meizu Pro 6 Plus – Exynos 8890
- Meizu 15 Plus – Exynos 8895
- Meizu M6s – Exynos 7872

UNISOC based phones

Capabilities : ? Partial extraction of data even when turned off, or turned on without being unlocked once since the boot.

? Brute-force password work partially

Code • Nokia C1 / C1 Plus

- Nokia C2 / C2 2nd Edition / C2 Tennen
- Nokia C3 / C5 Endi
- Nokia C10 / C20 / C21 / C21 Plus

- Itel Vision 1 / 1 Pro / 2 / 3
- Itel P37 / P40 / A49 / A60 / A70
- Itel Vision 1 / 1 Pro / 2 / 3
- Itel P37 / P40 / A49 / A60 / A70
- Moto E20
- Moto E22i
- Honor X5 / X5 Plus
- Ulefone Armor X7 / Note 8
- Blackview A80 / A70 / BV4900
- Doogee X95 / X96 Pro
- Nokia 3310 4G
- Nokia 8110 4G
- Nokia 110 4G / 105 4G
- Nokia 215 4G / 225 4G
- Nokia 5710 XpressAudio
- Alcatel MyFlip / Go Flip / A405DL
- Alcatel 3088
- Doro 7010 / 7030
- Jio Phone / Jio Phone 2 / Jio Bharat B1 / JioPhone Next
- Tecno Pop 5 / Pop 6 / Pop 7
- Infinix Smart 5 / Smart 6 / Smart 7 / Note 30i
- Symphony / Lava / Micromax : many entry models

END

This is a very interesting topic, if I have enough feed backs / engagement to this one I could make a tutorial in depth, there are old Cellebrite devices than can be bought on eBay, they won't work with the latest smartphones, but I could make a video to show how it works with at least old devices, remember :

<https://hackforums.net/showthread.php?tid=6290667>
<https://hackforums.net/showthread.php?tid=6292046>

Sources used to make this thread :
 (french) :

<https://polyope.net/wp-content/uploads/2025/04/Rapport-danalyse-des-capacites-de-Cellebrite-fevrier-2025-special-Android.pdf>

(english) :

<https://osservatorionessuno.org/blog/2025/03/a-deep-dive-into-cellebrite-android-support-as-of-february-2025/>

?rew - April 21, 2025, 12:10 pm

Strange that the same document from 2024 is now referenced as 2025.
 This is very old April 2024.

Also the device posted in your image are old Ufed touch 2 devices that most do not use for cracking. These are more so cooperated give me your password and I will image the device. It can do the lockpick exploit on s7 and older models but these went out of touch in 2019ish.
 Alot of the data you reference was leaked in 2024 and is old outdated.

Since this is public and they posted it here is a video
<https://youtu.be/IBEznORkt5I?t=18>

Notice at the timestamp what the device is doing and what the device is connected to. It will not be the ufed touch 2.

Another video:
<https://youtu.be/t41qM8GN23M?t=136>

notice what is on the screen at the timestamp, What is the software called on that screen.

DramaKing - April 21, 2025, 12:12 pm

It's crazy that so many Samsungs can be exploited. Glad that I have a Pixel (or did).

?rew - April 21, 2025, 12:15 pm

(Apr 21, 2025 12:12 PM)DramaKing Wrote: [\[CITE\]](#) It's crazy that so many Samsungs can be exploited. Glad that I have a Pixel (or did).

Pixel is vulnerable just as much as Samsung was

DramaKing - April 21, 2025, 12:16 pm

(Apr 21, 2025 12:15 PM)?rew Wrote: [\[CITE\]](#) Pixel is vulnerable just as much as Samsung was
You got a different list to back that up? I at least set a decent password.

Bastille - April 21, 2025, 12:24 pm

(Apr 21, 2025 12:10 PM)?rew Wrote: [\[CITE\]](#) Strange that the same document from 2024 is now referenced as 2025.

This is very old April 2024. A lot of the data you reference was leaked in 2024 and is old outdated. There is a 2024 version here which is numbered 7.69 :

<https://discuss.grapheneos.org/d/14344-cellebrite-premium-july-2024-documentation>

The new version is numbered 7.73, there actually some differences, for example here : Table 1 : Android OS Access Support Matrix - Unlocked devices [number version]

Pixel 9 has been added on the list too.

(Apr 21, 2025 12:10 PM)?rew Wrote: [\[CITE\]](#) Also the device posted in your image are old Ufed touch 2 devices that most do not use for cracking. These are more so cooperated give me your password and I will image the device. It can do the lockpick exploit on s7 and older models but these went out of touch in 2019ish.

Thanks for the info, I saw you posting on this thread

<https://hackforums.net/showthread.php?tid=6284764> and saw on your profile that you were into this field

I don't expect getting my hands on an expensive and un-buyable 2025 model, old and cheap models are good for what I need, just play with

ttbr0 - April 22, 2025, 12:28 am

(Apr 21, 2025 11:18 AM)Bastille Wrote: [\[CITE\]](#) This topic is very interesting, and the vulnerabilities now rely more on hardware instead of software (Android - keeping your smartphone up to date do not protect you anymore).

where did you get this impression?

Hopsin - April 22, 2025, 3:25 am

(Apr 21, 2025 12:12 PM)DramaKing Wrote: [\[CITE\]](#) It's crazy that so many Samsungs can be exploited. Glad that I have a Pixel (or did).

It doesn't matter what you have. Everything is exploitable.

Bastille - April 22, 2025, 9:36 am

(Apr 22, 2025 12:28 AM)ttbr0 Wrote: [\[CITE\]](#) where did you get this impression?

Info from this video (french). The guy has worked many years for LE, specialized in mobile forensic
:

Feel free to enable the translation, or you can use the transcript function and then paste to an LLM and ask for a translation or résumé

(Apr 22, 2025 03:25 AM)Hopsin Wrote: [\[CITE\]](#) It doesn't matter what you have. Everything is exploitable.

So far, the only combo that seems bullet proof against Cellebrite (and probably Graykey) is the Google Pixel (not sure if all versions are concerned, or only the latest such as 8 and 9), with GraphenOS.

(Apr 21, 2025 12:15 PM)?rew Wrote: [\[CITE\]](#) Pixel is vulnerable just as much as Samsung was
So far, latest Pixel with GraphenOS seem bullet proof

Mooooookie - April 22, 2025, 11:52 am

(Apr 22, 2025 09:36 AM)Bastille Wrote: [\[CITE\]](#) So far, latest Pixel with GraphenOS seem bullet proof
So from what you understand, the Pixel 9 Pro is safe?

Bastille - April 22, 2025, 12:13 pm

(Apr 22, 2025 11:52 AM)Mooooookie Wrote: [\[CITE\]](#) So from what you understand, the Pixel 9 Pro is safe?

Only if Pixel 9 Pro is running under GraphenOS, otherwise if it's under Android it's vulnerable, it's not in my thread I'll add it.

That said, there are different cases, for example :

- BFU = Before First Unlock, if you've turned off your phone and LE take it to extract information, they'll get access to partial information only
- AFU = After First Unlock, if you're arrested, your phone is on and you were using it recently (at least one time after turning it on) they'll be able to extract more data, because the unlock pass is in the memory that is accessible to Cellebrite (they will get access to : messages, photos, apps, encrypted data, and even sometimes the passcode to unlock it).

Take a look here : FFS = Full File System (extraction) / BF = Brute Force

?rew - April 22, 2025, 3:17 pm

(Apr 21, 2025 12:16 PM)DramaKing Wrote: [\[CITE\]](#) You got a different list to back that up? I at least set a decent password.

Most are behind NDA but you can find "lists" look into Premium not UFED.

Here an old video on the subject

<https://cellebrite.com/en/advance-your-toughest-investigations-with-cellebrite-advanced-services/>

(Apr 22, 2025 09:36 AM)Bastille Wrote: [\[CITE\]](#) Info from this video (french). The guy has worked

many years for LE, specialized in mobile forensic :

Feel free to enable the translation, or you can use the transcript function and then paste to an LLM and ask for a translation or résumé

So far, the only combo that seems bullet proof against Cellebrite (and probably Graykey) is the Google Pixel (not sure if all versions are concerned, or only the latest such as 8 and 9), with GraphenOS.

So far, latest Pixel with GraphenOS seem bullet proof
Depends but when I left Pixel was very exploitable. You are right about the hardware being the exploit point for most examples used.
Most do not really want to advertise it being exploited due to the cat and mouse game so sometimes it's better to not announce GraphenOS is exploitable and let people think it isn't.

ttbr0 - April 23, 2025, 12:56 am

(Apr 22, 2025 09:36 AM) Bastille Wrote: [\[CITE\]](#) Info from this video (french). The guy has worked many years for LE, specialized in mobile forensic :

Feel free to enable the translation, or you can use the transcript function and then paste to an LLM and ask for a translation or résumé

So far, the only combo that seems bullet proof against Cellebrite (and probably Graykey) is the Google Pixel (not sure if all versions are concerned, or only the latest such as 8 and 9), with GraphenOS.

So far, latest Pixel with GraphenOS seem bullet proof
I've read the entire translated transcript and quickly looked through the Graphene OS security hardening. Usually I am very skeptical about people's knowledge about these very niche and highly specialized topics but it seems that this person is very very well informed. I can't speak for hardware security because I am not educated enough about that area. What I can say is that hardware attacks are not the only thing involved here. Yes, hardware security underlies the entire system but it is not the only vector of attack and there have been many many cases where it wasn't. I've not seen the security enhancements of Graphene OS before, but I have seen some of their contributions here and there on my feeds. It's also safe to say that the team working on Graphene OS is incredibly technically competent and know what they are doing from a glance at their additional security features. But it doesn't mean that they are impenetrable. Just because Cellebrite and Graykey are unable to crack them doesn't mean someone else can't. I would wager that it has been exploited or will be exploited soon. As good as the Graphene OS are, attackers are also, if not more, capable themselves.