CELLEBRITE ZERO-DAY EXPLOIT USED TO TARGET PHONE OF SERBIAN STUDENT ACTIVIST

RESEARCH BRIEFING

AMNESTY INTERNATIONAL

CONTENTS

This briefing documents how a Cellebrite zero-day exploit was used to target the phone of a Serbian student activist. The attack closely matches the form of attack that we previously documented in a report, “A Digital Prison”: Surveillance and the suppression of civil society in Serbia, published in December 2024. The briefing is the result of a collaboration between Amnesty International’s European Regional Office and the Amnesty International Security Lab.

Cover photo: Composite image created by Amnesty International using photos provided by SviĆe and Dragan Gmizic.

INTRODUCTION

Amnesty International's Security Lab, in collaboration with Amnesty's European Regional Office, has uncovered a new case of misuse of a Cellebrite product to break into the phone of a youth activist in Serbia. The attack closely matches the form of attack that we previously documented in a report, 'A Digital Prison', published in December 2024. This new case provides further evidence that the authorities in Serbia have continued their campaign of surveillance of civil society in the aftermath of our report, despite widespread calls for reform, from both inside Serbia and beyond, as well as an investigation into the misuse of its product, announced by Cellebrite.

Though not documented in this blog post, Amnesty International has also found evidence of at least two further cases of misuse of Cellebrite against civil society (beyond the ones noted in the report), suggesting that the practice remains widespread and that Serbia's Security-Information Agency (Bezbedonosno-informativna agencija – BIA) and the Serbian security services remain confident that they can continue using such oppressive tactics with impunity.

In a statement published on 25 February 2025, Cellebrite announced that it has suspended the use of its products by "relevant customers" in Serbia following Amnesty International's December 2024 report, which documented widespread misuse of Cellebrite's technology by Serbian authorities. The latest findings of further abuses make these suspensions a necessary and crucial first step in halting the ongoing and unlawful misuse of the company's products.

ZERO-DAY EXPLOIT TARGETING ANDROID USB KERNEL DRIVERS IDENTIFIED IN-THE-WILD

This technical briefing provides a detailed analysis of how the Android phone of one student protester was exploited and unlocked by a sophisticated zero-day exploit chain targeting Android USB drivers, developed by Cellebrite. Amnesty International first found traces of this Cellebrite USB exploit used in a separate case in mid-2024.

These most recent findings show the ongoing harms from the continued misuse of Cellebrite's advanced mobile phone extraction tools, even after widely published evidence of abuses. Since the exploits identified in this research target core Linux kernel USB drivers, the vulnerability is not limited to a particular device or vendor and could impact over a billion Android devices.

In 2024, the Security Lab shared technical evidence about this zero-day exploit chain with industry partners, including Google's Threat Analysis Group. These leads enabled Google security researchers to identify at least three zero-day vulnerabilities likely exploited as part of this Cellebrite exploit chain. The first vulnerability, CVE-2024-53104, an out-of-bound write in the USB Video Class (UVC) driver, was patched in the February 2025 Android Security Bulletin.

Additional vulnerabilities CVE-2024-53197, and CVE-2024-50302 have been patched upstream in the Linux kernel but have not yet been included in an Android Security Bulletin. An initial technical analysis of the exploit and vulnerabilities is shared in Section 3 below.

Amnesty International wishes to thank the student activist targeted in this campaign for sharing his story and all partners who supported this research, including the Balkan Investigative and Reporting Network (BIRN) and SHARE Foundation in Belgrade.

Amnesty International extends special thanks to Benoît Sevens of Google's Threat Analysis Group for his invaluable contribution to this investigation, and his work identifying the underlying USB vulnerabilities exploited in this attack. The Security Lab is also grateful to the Android Security and Privacy team for their active engagement on addressing digital security risks impacting civil society.

1. UNCOVERING A HIGHLY SOPHISTICATED USB ZERO-DAY EXPLOIT CHAIN

Over the past year, the Security Lab has supported numerous protestors and other individuals worldwide who suspect that their mobile phones and personal data were accessed or extracted without consent or judicial approval. Amnesty International's forensic research on these cases has enabled us to build a detailed understanding of the technical methodologies used in mobile forensic products, such as those developed by Cellebrite, and similar companies.

Such research can also allow, in some cases, for the identification of software exploits which are being actively misused against civil society, with an associated negative human rights impact. Patching these vulnerabilities can reduce ongoing harms, pending action from mobile forensic vendors to limit the illegitimate use of their products.

Amnesty International has previously documented how a zero-day exploit targeting Qualcomm Android devices (CVE-2024-43047) was used to extract data from the phone of a Serbian activist in December 2023. Evidence gathered by the Security Lab enabled **Google Project Zero to identify the underlying** kernel vulnerability, which was patched by Qualcomm in **October 2024**.

This technical report describes a new Cellebrite zero-day exploit chain misused to covertly unlock the phone of a Serbia student activist. Amnesty International's Security Lab first discovered evidence of Cellebrite's USB zero-day exploit chain, when in mid-2024, it was used to unlock an Android device in a separate case outside Serbia.

The exploit, which targeted Linux kernel USB drivers, enabled Cellebrite customers with physical access to a locked Android device to bypass an Android phone's lock screen and gain privileged access on the device. As the exploit targets core Linux kernel USB drivers, the impact is not limited to a particular device or vendor and could affect a very wide range of devices. The same vulnerabilities could also expose Linux computers and Linux-powered embedded devices to physical attacks, although there is no evidence of this exploit chain has been designed to target non-Android Linux devices.

This case highlights how real-world attackers are exploiting Android's USB attack surface, taking advantage of the broad range of legacy USB kernel drivers supported in the Linux kernel. Android vendors must urgently strengthen defensive security features to mitigate threats from untrusted USB connections to locked devices.

Upstream patches for additional vulnerabilities in this chain will be made available by Android vendors over the coming months. Amnesty International is publishing this research now to raise awareness about how this USB attack surface is being exploited in the wild.

As the attack described in this blog requires physical access to the device and in-depth engineering efforts, the risk of reuse of this exploit is relatively low. However, to mitigate this risk, we are holding off sharing the technical details about the identified vulnerabilities until security patches are available from all major Android vendors. We are also not disclosing all associated crash logs and exploitation artifacts at this time.

These findings also highlight the value of device vendors and industry researchers working closely with civil society to identify and fix vulnerabilities impacting activists and journalists, helping to protect all their users in the process. Over the past six months, at least six zero-day vulnerabilities

– exploited in the wild – have been found through collaboration with civil society security researchers from **Citizen Lab** and **Amnesty International**.

2. HOW DIGITAL FORENSICS TOOLS HAVE BEEN USED AGAINST CIVIL SOCIETY IN SERBIA

On 16 December 2024, Amnesty International's Security Lab and Europe Regional Office published "A Digital Prison": Surveillance and the Suppression of Civil Society in Serbia". The report documented how the Serbian police and intelligence authorities are using advanced phone spyware alongside mobile phone forensic products to unlawfully target journalists, environmental activists and others critical of government policies in a covert surveillance campaign.

One of the most explosive findings was to show how mobile forensic products made by the Israeli company Cellebrite are being widely misused to extract data from mobile devices belonging to journalists and activists. In response to our findings, Cellebrite stated that "We are investigating the claims made in this report. Should they be validated, we are prepared to impose appropriate sanctions, including termination of Cellebrite's relationship with any relevant agencies."

The report also prompted strong responses inside Serbia, where an association of 10 civil society organizations filed criminal charges against police and intelligence authorities over unlawful surveillance and formally requested separate investigations by the Ombudsman's Office and the Data Protection Commissioner. The Serbian Prosecutor for High Technological Crime formally registered the case in January 2025.

In January 2025, one month after the publication of the report, the Security Lab received a request to test the device of a youth protester who had been arrested and detained by the Serbian Security-Information Agency (Bezbedonosno-informativna agencija – BIA) on 25 December 2024, following large student protests in Belgrade. The circumstances of his arrest, and the behaviour of the BIA officers, strongly matched the *modus operandi* that was used against protesters and that we documented in our report in December. A forensic investigation of the device conducted in January confirmed the use of Cellebrite on the student activist's phone. The details of the arrest and attack on the phone of the protester are included in Section 3, below.

In this blog post, we provide a summary of the events around the arrest and targeting of the student protestor. In common with cases documented in our December report, Cellebrite UFED was used on the activist's phone without his knowledge or consent, and outside a legally sanctioned investigation. The seemingly routine use of Cellebrite software against people for exercising their rights to freedom of expression and peaceful assembly can never be a legitimate aim, and therefore is in violation of human rights law. (For a more detailed analysis of Serbia's legal framework around digital surveillance, and the human rights impacts of the use of Cellebrite against civil society, see Chapters 7 and 8.2 of A Digital Prison).

3. STUDENT ACTIVIST DETAINED BY PLAIN CLOTHES OFFICERS AT PROTEST

"Vedran" (name has been changed to protect the student's security, privacy and confidentiality) is a 23-year old student activist who regularly participates in the ongoing student protests in Belgrade. Although he is loosely associated with several youth organizations he considers himself a part of the broader peaceful student protest movement that has swept Serbia since November 2024.

On 25 December 2024, "Vedran" wanted to check out an "open meeting with young people" which was organized by the ruling Serbian Progressive Party in Belgrade.

At the entrance to the protest point, "Vedran" left his vuvuzela with the security. After a while (at around 17:30 CET), seven men in plain clothes approached him and forced him into a car. Despite his demands that they identify themselves, they did not introduce themselves and acted aggressively. They asked him why he was there and why he carried a vuvuzela and demanded that he show them his phone. He refused and was then driven to a police station in Sava Mala (part of Belgrade).

"Vedran" told Amnesty International that as soon as he entered the police station, around 18:30 local time, he switched off his telephone and handed it over to the officers. He was led to an office on the 1st floor and, for the next six hours, questioned by four men in civilian clothes who never introduced themselves.

His phone was returned to him around 00:45 AM. It was switched off.

3.1 CELLEBRITE EXPLOITS USED TO UNLOCK PHONE BEFORE ATTEMPTED INFECTION WITH ANDROID APP

Amnesty International's Security Lab performed a forensic analysis on "Vedran's" Samsung Galaxy A32 to check if the device was tampered with while "Vedran" was detained at the police station.

The forensic analysis found clear evidence of exploitation which Amnesty International can confidently attribute to the use of Cellebrite's UFED product. The logs also show that the Cellebrite product enabled the authorities to successfully gain privileged root access to the phone and to unlock the device.

Timestamp (Local Time)	Event
2024-12-25 18:36:10	"Vedran" turned his phone off.
2024-12-25 20:01:14	Phone turned on for the first time in police station.
2024-12-25 20:22:13	Phone turned on again at police station
2024-12-25 20:24:37	Emulated USB device (consistent with Cellebrite *Turbo Link)* connected to phone.
2024-12-25 20:28:38	Forensic traces of successful Cellebrite exploit and achieving code execution as the root user.
2024-12-25 20:30:11	Additional traces of Cellebrite activity on device.
2024-12-25 20:37:15	Traces show phone screen unlocked.

2024-12-25 20:37:59	Phone reboot triggered through Android shell

Table 1 - Forensic traces of Cellebrite use on the protesters Android device.

Amnesty International found evidence that the Serbian authorities attempted to install an unknown Android application after the phone was unlocked with Cellebrite.

Due to limited forensic logs, it was not possible to identify the specific Android app the authorities intended to install. However, this attempt to covertly install an Android app after using Cellebrite to unlock it is consistent with the previous cases of NoviSpy spyware infections documented by Amnesty International.

Timestamp (Local Time)	Event
2024-12-25 20:42:54	Traces showing phone was turned on again 5 minutes after reboot triggered
2024-12-25 20:55:49	Google Chrome app opened on the phone
2024-12-25 20:56:03	Permission granted to install APK with Chrome
2024-12-25 20:56:22	Android package installer opened with biometric/pin prompt. App installation appears to have been blocked.
2024-12-25 20:58:33	Traces of activity in the Samsung My Files app which may indicate the attackers cleaning up.
2024-12-25 21:13:18	Forensic traces of additional Cellebrite exploitation and code execution as **root** user. This may be an attempt to re-run an alternative Cellebrite workflow such as performing an After-First-Unlock extraction flow.

Table 2 - Attempts to install a side-loaded Android package after unlocking with Cellebrite.

After the failed attempts to install the APK, the forensic evidence shows new attempts to exploit the phone with Cellebrite UFED. These traces begin with the copying of Cellebrite's **falcon** tool to the phone. This may indicate a new attempt to exploit the phone with an *Unlocked* flow.

Timestamp (Local Time)	Event
2024-12-25 21:26:17	Phone rebooted
2024-12-25 21:31:38	Cellebrite **falcon** binary copied onto phone by ADB shell user
2024-12-25 21:38:55	Kernel OOPS when trying to **kfree** memory from Linux Transcendent Memory feature in *frontswap_tmem_e+0xc8/0x1b0*.
2024-12-25 21:47:01	Kernel OOPS when handling USB HID events.
2024-12-25 21:50:03	Forensic traces of successful Cellebrite exploitation and code execution as **root** user.
2024-12-25 21:53:59	Additional traces of Cellebrite UFED dropping files with **root** privileges.
2024-12-25 21:58:59	Trace of various shell commands including **find**, **grep** running on the device.

Table 3 - Traces of additional exploitation attempts involving the Cellebrite falcon binary.

The second round of exploitation with Cellebrite's falcon binary appears to have been successful as various post-exploitation commands were run on the device. It is unclear if the logs related to the Linux *Transcendent Memory* code are linked to exploitation of this driver or an unrelated artifact of kernel memory corruption.

3.2 ANDROID USB ZERO-DAY VULNERABILITIES EXPLOITED TO UNLOCK SAMSUNG ANDROID PHONE

The previous tables outlined some of the exploitation traces identified on the device. Determining the exact vulnerabilities exploited in a memory corruption attack can often be challenging, especially post-incident, due to the lack of detailed on-device logging.

However, in this case, Amnesty International has high confidence that the following forensic logs provide clear evidence of a Cellebrite USB exploit chain. While we are presenting logs specific to the most recent Serbian case, the patterns observed—including associated crashes—align with similar cases identified over the past year.

The attack involves the connection of various USB peripherals. The "Video Device" was connected during the initial stages of the exploit. The other devices show repeated connections indicating repeated stages of exploitation needed to disclose kernel memory and groom kernel memory as part of the exploitation.

It is unclear if each device listed below was part of the successful exploitation chain. As the attack occurs in before Before-First-Unlock, the attackers may need to actively fingerprint the kernel to determine which, if any exploit chain may be compatible:

Event	Notes
USB hub connected	
USB "Video Device" connected	VID: 0x04f2 PID: 0xb071 (Device: UVC Webcam / Chicony CNF7129).
USB "Sound Device" connected	VID: 0x041e PID: 0x3000 (Device: SoundBlaster Extigy). Repeated connections over a span of 30 seconds.
USB "Sound Device" connected	VID: 0x0763 PID: 0x2012. (Device: M-Audio Fast Track Pro). Repeated connections over a span of 30 seconds
USB "HID Device" connected	VID: 0x045e PID: 0x076c (Device: Comfort Mouse 4500). Repeated connections over a span of 30 seconds.
USB HID touch pad connected	VID: 0x1130 PID: 0x3101 (Device: Anton Touch Pad). Repeated connections over a span of 30 seconds.
Successful code execution as root	Code execution observed approx. 10 seconds after HID device connection

Table 4

All of the connected USB devices appear to be emulated in software via a Cellebrite hardware dongle. Cellebrite's Premium UFED or Inseyets product, which supports device unlocking, utilizes a separate "Turbo Link" adapter, which may be used to facilitate such hardware-based attacks.

The device names listed in the table—such as “Video Device” or “Sound Device”—are the actual product names specified in the corresponding USB device descriptors. Additionally, the USB device version numbers for all detected peripherals were uniformly set to the constant “12.34”, a strong indicator of emulation rather than genuine hardware.

```
USB device attached: vidpid 04f2:b071 mfg/product/ver/serial Video/Video Device/12.34/00001
hasAudio/HID/Storage: false/false/false
USB device attached: vidpid 041e:3000 mfg/product/ver/serial Sound/Sound Device/12.34/00001
hasAudio/HID/Storage: true/false/false
USB device attached: vidpid 0763:2012 mfg/product/ver/serial Sound/Sound Device/12.34/00001
hasAudio/HID/Storage: false/false/false
USB device attached: vidpid 0763:2012 mfg/product/ver/serial Sound/Sound Device/12.34/00001
hasAudio/HID/Storage: false/false/false
USB device attached: vidpid 0763:2012 mfg/product/ver/serial Sound/Sound Device/12.34/00001
hasAudio/HID/Storage: false/false/false
USB device attached: vidpid 0763:2012 mfg/product/ver/serial Sound/Sound Device/12.34/00001
hasAudio/HID/Storage: false/false/false
USB device attached: vidpid 0763:2012 mfg/product/ver/serial Sound/Sound Device/12.34/00001
hasAudio/HID/Storage: false/false/false
USB device attached: vidpid 0763:2012 mfg/product/ver/serial Sound/Sound Device/12.34/00001
hasAudio/HID/Storage: false/false/false
USB device attached: vidpid 0763:2012 mfg/product/ver/serial Sound/Sound Device/12.34/00001
hasAudio/HID/Storage: false/false/false
USB device attached: vidpid 0763:2012 mfg/product/ver/serial Sound/Sound Device/12.34/00001
hasAudio/HID/Storage: false/false/false
USB device attached: vidpid 0763:2012 mfg/product/ver/serial Sound/Sound Device/12.34/00001
hasAudio/HID/Storage: false/false/false
USB device attached: vidpid 0763:2012 mfg/product/ver/serial Sound/Sound Device/12.34/00001
hasAudio/HID/Storage: false/false/false
USB device attached: vidpid 0763:2012 mfg/product/ver/serial Sound/Sound Device/12.34/00001
hasAudio/HID/Storage: false/false/false
USB device attached: vidpid 0763:2012 mfg/product/ver/serial Sound/Sound Device/12.34/00001
hasAudio/HID/Storage: false/false/false
USB device attached: vidpid 0763:2012 mfg/product/ver/serial Sound/Sound Device/12.34/00001
hasAudio/HID/Storage: false/false/false
USB device attached: vidpid 0763:2012 mfg/product/ver/serial Sound/Sound Device/12.34/00001
hasAudio/HID/Storage: false/false/false
USB device attached: vidpid 0763:2012 mfg/product/ver/serial Sound/Sound Device/12.34/00001
hasAudio/HID/Storage: false/false/false
USB device attached: vidpid 0763:2012 mfg/product/ver/serial Sound/Sound Device/12.34/00001
hasAudio/HID/Storage: false/false/false
USB device attached: vidpid 0763:2012 mfg/product/ver/serial Sound/Sound Device/12.34/00001
hasAudio/HID/Storage: true/false/false
USB device attached: vidpid 045e:076c mfg/product/ver/serial hid/HID
Device/12.34/fedcba9876543210 hasAudio/HID/Storage: false/true/false
```

The serial number of the HID USB device was set to 33117733, which again indicates the device ID and serial numbers were emulated as part of an exploit attempt, rather than being a legitimate USB device.

```
<6>[  350.950690]  (1)[159:kworker/1:1]usb 1-1.1: udev->lpm_capable=0
<6>[  350.950737]  (1)[159:kworker/1:1]usb 1-1.1: usb_enumerate_device
<6>[  350.981150]  (1)[159:kworker/1:1]usb 1-1.1: vid:0x45e, pid:0x76c
<6>[  350.981182]  (1)[159:kworker/1:1]usb 1-1.1: product:HID Device,
manufacturer:hid
<6>[  350.981196]  (1)[159:kworker/1:1]usb 1-1.1: New USB device found,
idVendor=045e, idProduct=076c
<6>[  350.981205]  (1)[159:kworker/1:1]usb 1-1.1: New USB device
strings: Mfr=1, Product=2, SerialNumber=3
<6>[  350.981214]  (1)[159:kworker/1:1]usb 1-1.1: Product: HID Device
<6>[  350.981222]  (1)[159:kworker/1:1]usb 1-1.1: Manufacturer: hid
<6>[  350.981230]  (1)[159:kworker/1:1]usb 1-1.1: SerialNumber:
33117733
```

The USB device ID and vendor ID provided in the USB device descriptor, are used by the Linux kernel USB subsystem to determine which kernel driver will handle the connected USB device. Unfortunately, due to the extensive range of supported USB devices, and the necessity of accommodating legacy hardware and non-compliant implementations, the Linux USB stack presents a large attack surface. This includes numerous drivers and less-tested code paths that a local attacker could potentially exploit.
To better understand the Cellebrite exploit chain, we will now analyse each emulated USB device in turn, identifying the corresponding kernel drivers that may have been exploited during the attack.

"VIDEO DEVICE" (0XB071)

The *Video Device* USB device specified a USB ID pair *(VID: 0x04f2 PID: 0xb071)* which is registered as a Chicony CNF7129 UVC Webcam. This product ID is handled by the Linux USB Video Class (UVC) driver.

This specific USB device ID can reach a custom kernel code path, termed a quirk, called "UVC_QUIRK_RESTRICT_FRAME_RATE". Revealingly this is the only USB device ID which triggers this quirk, suggesting that the exploit targets a vulnerability introduced in that specific quirk code. The quirk, or non-standard coded path to handle this USB device was introduced in 2010, almost 15 years ago.

```
/* Chicony CNF7129 (Asus EEE 100HE) */
{ .match_flags         = USB_DEVICE_ID_MATCH_DEVICE
| USB_DEVICE_ID_MATCH_INT_INFO,
  .idVendor      = 0x04f2,
  .idProduct           = 0xb071,
  .bInterfaceClass     = USB_CLASS_VIDEO,
  .bInterfaceSubClass  = 1,
  .bInterfaceProtocol  = 0,
  .driver_info         = UVC_INFO_QUIRK(UVC_QUIRK_RESTRICT_FRAME_RATE)
},
```

These artifacts narrowed down a very small area of kernel code, which likely introduces an exploitable memory corruption vulnerability. Benoît Sevens of Google Threat Analysis Group found that this code path allows an out-of-bound write when parsing frames of type UVC_VS_UNDEFINED in *uvc_parse_format()*. The vulnerability was patched upstream in the Linux kernel in November 2024 and assigned CVE-2024-53104. The patch was included in the February 2025 Android Security Bulletin protecting all patched devices from code execution using this this entire USB exploit chain.

"SOUND DEVICE" (0X3000)

The next USB device, a "Sound Device" (VID: 0x041e PID: 0x3000) imitates a Creative Extigy USB sound card. The Linux ALSA USB-sound driver which handles this device also has a quirk, loading specific code for handling the initialization a set of non-standard Extigy and Mbox sound cards including Extigy devices with this particular device ID.

```
int snd_usb_apply_boot_quirk(struct usb_device *dev,
                             struct usb_interface *intf,
                             const struct snd_usb_audio_quirk *quirk,
                             unsigned int id)
{
        switch (id) {
```

```
        case USB_ID(0x041e, 0x3000):
                /* SB Extigy needs special boot-up sequence */
                /* if more models come, this will go to the quirk list.
*/
                return snd_usb_extigy_boot_quirk(dev, intf);
```

The quirk code in "snd_usb_extigy_boot_quirk" function reloads and copies the USB device descriptor during its custom device initialization code. A malicious emulated Extigy or Mbox device can exploit this quirk code by providing an invalid USB device descriptor during the "usb_get_descriptor()" call, where the descriptor has a bNumConfigurations value that exceeds the initial value sent by the USB device during first connection in "usb_get_configuration()".

```
static int snd_usb_extigy_boot_quirk(struct usb_device *dev, struct
usb_interface *intf)

{
---
    dev_dbg(&dev->dev, "sending Extigy boot sequence...\n");
    /* Send message to force it to reconnect with full interface. */
    err = snd_usb_ctl_msg(dev, usb_sndctrlpipe(dev,0),
                    0x10, 0x43, 0x0001, 0x000a, NULL, 0);
    if (err < 0)
        dev_dbg(&dev->dev, "error sending boot message: %d\n", err);
    err = usb_get_descriptor(dev, USB_DT_DEVICE, 0,
            &dev->descriptor, sizeof(dev->descriptor));
    config = dev->actconfig;
    if (err < 0)
        dev_dbg(&dev->dev, "error usb_get_descriptor: %d\n", err);
```

Benoît Sevens of Google's Threat Analysis Group identified that this vulnerability could lead to out-of-bounds accesses later, e.g. in usb_destroy_configuration if the "dev->config" member of the device is corrupted, again allowing for remote code execution. The vulnerability in the quirk code was patched upstream in November 2024 and assigned CVE-2024-53197.

"SOUND DEVICE" NO. 2 (0X2012)

The second "Sound Device" (VID: 0x0763 PID: 0x2012) again has a specific quirk code applied when the USB device is loaded in fasttrackpro_skip_setting_quirk(). This device is loaded immediately after the malicious Extigy device.

```
/* fasttrackpro usb: skip altsets incompatible with device_setup */
if (chip->usb_id == USB_ID(0x0763, 0x2012))
      return fasttrackpro_skip_setting_quirk(chip, iface, altno);
```

Interestingly, USB device connection logs seen during the exploitation indicated that the USB device descriptor of the malicious Extigy device, is apparently remapped as a Fasttrack Pro device *while* loaded in the kernel.

Timestamp	Seq Num	Action	Product	Device Path
20:26:24.932	6405	add	41e/3000/1234	/1-1/1-1.4/1-1.4:1.0

20:26:24.944	6406	add	763/2012/1234	/1-1/1-1.4/1-1.4:1.1
20:26:25.176	6408	remove	763/2012/1234	/1-1/1-1.4/1-1.4:1.0
20:26:25.177	6409	remove	763/2012/1234	/1-1/1-1.4/1-1.4:1.1

Table 5 - Extigy Sound Card device descriptor corrupted while connected to phone.

The device path includes the USB bus number and USB device number or DEVNUM, indicating the exact bus and path the kernel uses to communicate with the device.

In the table above we can see that the two different sound card devices (*0x3000* and *0x2012)* were added. Around 0.2 seconds later the kernel logs show that two 0x2012 devices are removed. The first and third entry in the table both show the same device path "1-1.4:1.0". These logs suggest that the attackers were able to use CVE-2024-53197 to successfully overwrite the original device descriptor *0x3000* with an arbitrary USB descriptor containing the 0x2012 device.

It is unclear why the FastTrackPro (0x2012) device was chosen as the target. The attacker may be able to use properties of the new FastTrackPro to confirm that the memory corruption primitive CVE-2024-53197 is functional on this device.

ANTON TOUCH PAD DEVICE (0X3101)

The next connected device – where we did not observe the attacker supplied device name – emulated a multitouch HID USB input device. It is identified in the Linux kernel as an Anton Touchpad. The code for this device was introduced 11 years ago.

```
#define USB_VENDOR_ID_ANTON             0x1130
#define USB_DEVICE_ID_ANTON_TOUCH_PAD           0x3101
```

Again, the kernel use a non-standard configuration for this device, and sets a driver option named "`MT_CLS_EXPORT_ALL_INPUTS`" when loading devices of this type. The same option is only passed to one other device type.

```
/* Anton devices */
{ .driver_data = MT_CLS_EXPORT_ALL_INPUTS,
       MT_USB_DEVICE(USB_VENDOR_ID_ANTON,
              USB_DEVICE_ID_ANTON_TOUCH_PAD) },
```

The driver then uses the "`MT_CLS_EXPORT_ALL_INPUTS`" option to **load two quirks for the device**, alongside setting an "export_all_inputs" flag.

```
{ .name = MT_CLS_EXPORT_ALL_INPUTS,
       .quirks = MT_QUIRK_ALWAYS_VALID |
              MT_QUIRK_CONTACT_CNT_ACCURATE,
       .export_all_inputs = true },
```

Benoît Sevens found this quirk and device configuration could be used to leak uninitalized kernel memory to a local attacker through special crafted HID reports. The memory disclosure issue was mitigated by zeroing the HID report buffer when it is allocated. This vulnerability was patched as **CVE-2024-50302**.

"HID DEVICE" (0X76C)

The final USB device connected during the exploitation flow was a "HID Device" (VID: 0x045e PID: 0x076c) which emulated a Microsoft Comfort Mouse 4500. As you will have guessed by now, this device also has a Linux kernel quirk, this time in the **USB HID device driver**.

```
#define USB_DEVICE_ID_MS_COMFORT_MOUSE_4500 0x076c
```

The quirk "**MS_DUPLICATE_USAGES**" is applied and again this quirk is only applied to this specific product and device ID. The relevant quirk code for this device was introduced into the Linux kernel almost 14 years ago.

```
{ HID_USB_DEVICE(USB_VENDOR_ID_MICROSOFT,
USB_DEVICE_ID_MS_COMFORT_MOUSE_4500),
               .driver_data = MS_DUPLICATE_USAGES },
```

The `MS_DUPLICATE_USAGES` quirk code is also **extremely simple**, with one line of extra kernel code to clear some clear data on the USB descriptor. It is unclear exactly what function this quirk plays as part of the chain.

```
        if (quirks & MS_DUPLICATE_USAGES)
                clear_bit(usage->code, *bit);
```

This emulated HID device was connected at least 42 times and was the final device connected immediately before the device shows signs of successful arbitrary code execution as root. The repeated connections may be attempts to groom kernel memory or trigger code execution.

LONG-TERM SECURITY RISKS FROM NON-MEMORY SAFE DEVICE DRIVERS

This USB exploit chain shows the long-tail risk of non-memory-safe Linux kernel code, particular the large amount of device driver code introduced to handle a range of non-standards compliant USB devices. Recent efforts to introduce memory-safe languages such as Rust in the Linux kernel provide a promising option to reduce such security issues in newly written device drivers. Other security mitigations, such as blocking the connection of new or untrusted USB hardware on a locked device, may provide more immediate defences against vulnerabilities in existing non-memory-safe kernel drivers.

4. CONCLUSION: AN URGENT NEED FOR INVESTIGATION INTO THE MISUSE OF DIGITAL FORENSICS TOOLS IN SERBIA

Amnesty International informed Cellebrite on 31 January 2025 about the continued misuse of their forensic products by the Serbian authorities. The additional case described here occurred on 25 December 2024, nine days after the publication of our report and almost one month *after* Amnesty International first provided Cellebrite with detailed evidence of misuse of their products. Cellebrite stated on 25 February that:

> **“After a review of the allegations brought forth by the December 2024 Amnesty International report, Cellebrite took precise steps to investigate each claim in accordance with our ethics and integrity policies. We found it appropriate to stop the use of our products by the relevant customers at this time.”**
> Statement from Cellebrite

While the statement and decision to stop the use of their products ‘by the relevant customers’ is welcome evidence that Cellebrite have taken steps to investigate and take action, it is not clear whether this latest case was included in their investigation. Furthermore, Cellebrite could not provide Amnesty International with additional information on the duration for which the customers have been suspended, nor what conditions or human rights protections are required before they will be allowed to use Cellebrite products again. The case reinforces the urgency for Cellebrite to introduce meaningful and effective safeguards to reduce the risk of their products enabling human rights abuses, including thorough review of their due diligence procedures; the implementation of technical mechanisms to limit the invasiveness of Cellebrite forensic tools; and to provide compensation and redress for the victims whose rights have been violated by the unlawful use of their products.

In light of this latest case of misuse of advanced digital technologies by Serbian authorities, all forensic and surveillance technology providers should suspend surveillance technology sales to Serbian authorities, due to a real risk of such tools being used as part of the ongoing crackdown on the protest movements. Vendors of IMSI catchers, spyware, and mobile forensic technology should suspend sales to BIA and other authorities in Serbia until a human rights compliant framework is in place to prevent further abuses.

In the light of the continued misuse of digital forensic tools for political purposes in Serbia and Cellebrite’s decision to halt the use of its product by some customers in the country, the Serbian authorities must – without further delay – investigate all reported cases of misuse of digital forensics tools against members of civil society and journalists in Serbia, put in place an effective and robust legal framework that prevents such abuses and provides independent control and oversight over surveillance practices. Finally, the authorities must provide effective remedy to victims of unlawful targeted surveillance and hold perpetrators to account for the violations.

For more detailed recommendations, see Chapter 9 of A Digital Prison.

Amnesty International shared the details of the case documented in this research with BIA and gave the agency an opportunity to respond to the findings before the publication of this briefing. BIA did not respond to the request.

APPENDIX: FULL TRACES OF USB EXPLOITATION ATTEMPTS

The following table shows traces of each USB connection and disconnection event which was seen while the youth activist's phone was exploited using Cellebrite UFED. There separate exploitation flows are evident, each beginning with the connection of a USB hub device and ending with its disconnection. While some devices such as the HID mouse (0x076c) are seen each flow, the UVC Webcam (0xb071) and the Extigy Sound Card (0x3000) are only seen in the second and third flows respectively.

The observed artifacts suggest that the Cellebrite UFED system attempted to trigger multiple related but distinct exploit chains in order the unlock the device. The vulnerability analysis above shows how both the UVC Webcam flow, and the Extigy Sound Card can flow can be used to corrupt kernel memory and gain arbitrary code execution.

A table showing traces of each USB connection and disconnection event which was seen while the youth activists phone was exploited using Cellebrite UFED can be viewed at: https://securitylab.amnesty.org/latest/2025/02/cellebrite-zero-day-exploit-used-to-target-phone-of-serbian-student-activist/

Amnesty International is a movement of 10 million people which mobilizes the humanity in everyone and campaigns for change so we can all enjoy our human rights. Our vision is of a world where those in power keep their promises, respect international law and are held to account. We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and individual donations. We believe that acting in solidarity and compassion with people everywhere can change our societies for the better.

Contact

info@amnesty.org

amnesty.org

facebook.com/AmnestyGlobal

@Amnesty

Amnesty International
Peter Benenson House
1 Easton Street
London WC1X 0DW, UK

Index: **EUR 70/9118/2025**
Publication: **February 2025**
Original language: **English**