

TRACK 1

HITBSECCONF

AMSTERDAM - 2021

The State of Mobile Security

Zuk Avraham (@ihackbanme)

Co-founder and CEO at ZecOps



Zuk Avraham
Security Researcher



zuk.av@zecops.com



[@ihackbanme](https://twitter.com/ihackbanme)

SAMSUNG

 **ZIMPERIUM**

 **zecOps**

Founder, Chairman
2010 - Present

Founder, CEO
2017 - Present



Everything Cyber, Mobile DFIR, Chess, Cooking

 **zecOps**



Smartphones



~3 billion users



Microphone

Camera

Emails

SMS

Pictures, Videos, ...



Our 2nd Factor!



Summer 2017: A Tale of a Sudden Reboot

- Oops. The phone just rebooted.
- Down the rabbit hole...
- Second panic
- Blocked from analyzing my own device



The Problem



- Phones are limited in what you can see
- Due to “privacy” we are not allowed to check if the device is ... private.
- We have local admin on our PCs and Macs - shouldn't we have similar access on our phones?

How bad is it? Android May 2021



ars TECHNICA SUBSCRIBE SEARCH SIGN IN

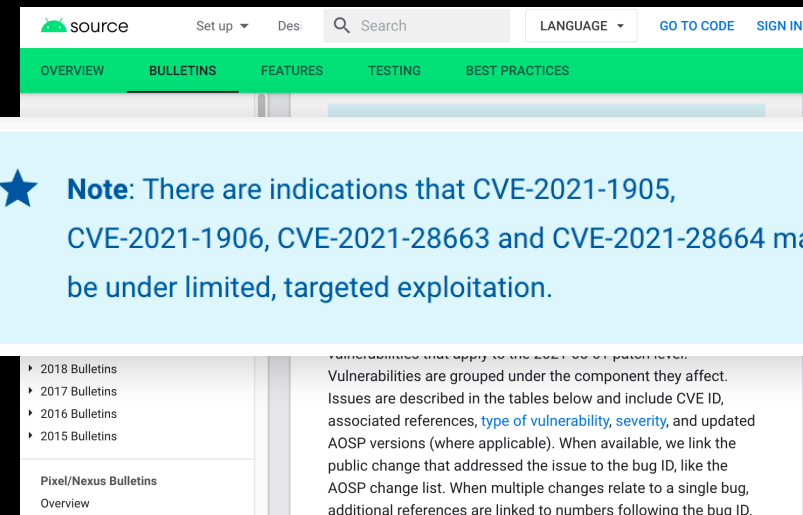
BETTER LATE THAN NEVER —

4 vulnerabilities under attack give hackers full control of Android devices

Google updates a 2-week-old security bulletin to say some vulnerabilities were 0-days.

DAN GOODIN - 5/19/2021, 11:45 PM

<https://arstechnica.com/gadgets/2021/05/hackers-have-been-exploiting-4-critical-android-vulnerabilities/>



source Set up Des Search LANGUAGE GO TO CODE SIGN IN

OVERVIEW BULLETINS FEATURES TESTING BEST PRACTICES

★ **Note:** There are indications that CVE-2021-1905, CVE-2021-1906, CVE-2021-28663 and CVE-2021-28664 may be under limited, targeted exploitation.

2018 Bulletins
2017 Bulletins
2016 Bulletins
2015 Bulletins

Pixel/Nexus Bulletins Overview

Vulnerabilities are grouped under the component they affect. Issues are described in the tables below and include CVE ID, associated references, **type of vulnerability**, **severity**, and updated AOSP versions (where applicable). When available, we link the public change that addressed the issue to the bug ID, like the AOSP change list. When multiple changes relate to a single bug, additional references are linked to numbers following the bug ID.

<https://source.android.com/security/bulletin/2021-05-01>

How bad is it? Android Jan 2021

The screenshot shows the Android Source website's security bulletin page for January 2021. At the top, there is a navigation bar with the Android logo, 'source', and links for 'Set up', 'Design', 'Search', 'ENGLISH', 'GO TO CODE', and 'SIGN IN'. Below this is a green navigation menu with 'OVERVIEW', 'BULLETINS', 'FEATURES', 'TESTING', and 'BEST PRACTICES'. A light blue callout box with a star icon contains the following text: **Note:** There are indications that CVE-2020-11261 may be under limited, targeted exploitation. Below the callout, the page content is visible, including a sidebar with a 'January Index' listing bulletins from 2020 to 2015, and a main content area with the heading 'details' and introductory text about security vulnerabilities for the 2021-01-01 patch level.

<https://source.android.com/security/bulletin/2021-01-01>

How bad is it? Android Jan 2021

★ **Note:** There are indications that CVE-2020-11261 may be under limited, targeted exploitation.



Dan Goodin
@dangoodin001

Replying to @maddiestone

"May be under limited, targeted exploitation" is vague to the point of being meaningless. I really wish Google and other companies wouldn't hedge like this when their customers are under attack. I know you have no control over this, Maddie. I just needed to get this off my chest.

9:14 AM · May 19, 2021 · TweetDeck

2 Retweets 1 Quote Tweet 21 Likes

<https://source.android.com/security/bulletin/2021-01-01>

How bad is it? iOS 12.1.4

- Didn't mention that these vulnerabilities were exploited in the wild...

Foundation

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: An application may be able to gain elevated privileges

Description: A memory corruption issue was addressed with improved input validation.

CVE-2019-7286: an anonymous researcher, Clement Lecigne of Google Threat Analysis Group, Ian Beer of Google Project Zero, and Samuel Groß of Google Project Zero

IOKit

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: An application may be able to execute arbitrary code with kernel privileges

Description: A memory corruption issue was addressed with improved input validation.

CVE-2019-7287: an anonymous researcher, Clement Lecigne of Google Threat Analysis Group, Ian Beer of Google Project Zero, and Samuel Groß of Google Project Zero

<https://support.apple.com/en-us/HT209520>

How bad is it? iOS 14.2

- No report ?
- No IOC



FontParser

Available for: iPhone 6s and later, iPod touch (7th generation), iPad Air 2 and later, and iPad mini 4 and later

Impact: Processing a maliciously crafted font may lead to arbitrary code execution. Apple is aware of reports that an **exploit for this issue exists in the wild**.

Description: A memory corruption issue was addressed with improved input validation.

CVE-2020-27930: Google Project Zero

Kernel

Available for: iPhone 6s and later, iPod touch (7th generation), iPad Air 2 and later, and iPad mini 4 and later

Impact: A malicious application may be able to execute arbitrary code with kernel privileges. Apple is aware of reports that an **exploit for this issue exists in the wild**.

Description: A type confusion issue was addressed with improved state handling.

CVE-2020-27932: Google Project Zero

Kernel

Available for: iPhone 6s and later, iPod touch (7th generation), iPad Air 2 and later, and iPad mini 4 and later

Impact: A malicious application may be able to disclose kernel memory. Apple is aware of reports that an **exploit for this issue exists in the wild**.

Description: A memory initialization issue was addressed.

CVE-2020-27950: Google Project Zero

<https://support.apple.com/en-us/HT211929>

HITB SECCONF
AMSTERDAM - 2021

How bad is it? iOS 14.4

- No report
- No IOC

Kernel

Available for: iPhone 6s and later, iPad Air 2 and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: A malicious application may be able to elevate privileges. Apple is aware of a report that this issue may have been actively exploited.

Description: A race condition was addressed with improved locking.

CVE-2021-1782: an anonymous researcher

WebKit

Available for: iPhone 6s and later, iPad Air 2 and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: A remote attacker may be able to cause arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

Description: A logic issue was addressed with improved restrictions.

CVE-2021-1871: an anonymous researcher

CVE-2021-1870: an anonymous researcher

<https://support.apple.com/en-us/HT212146>

How bad is it? iOS 14.5

- No report
- No IOC

WebKit Storage

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively **exploited**.

Description: A use after free issue was addressed with improved memory management.

CVE-2021-30661: yangkang(@dnpushme) of 360 ATA

<https://support.apple.com/en-us/HT212317>

How bad is it?

iOS 14.5.1

- No report
- No IOC

iOS 14.5.1 and iPadOS 14.5.1

Released May 3, 2021

WebKit

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: Processing maliciously crafted web content may lead to arbitrary code execution. **Apple is aware of a report that this issue may have been actively exploited.**

Description: A memory corruption issue was addressed with improved state management.

CVE-2021-30665: yangkang (@dnpushme)&zerokeeper&bianliang of 360 ATA

WebKit

Available for: iPhone 6s and later, iPad Pro (all models), iPad Air 2 and later, iPad 5th generation and later, iPad mini 4 and later, and iPod touch (7th generation)

Impact: Processing maliciously crafted web content may lead to arbitrary code execution. **Apple is aware of a report that this issue may have been actively exploited.**

Description: An integer overflow was addressed with improved input validation.

CVE-2021-30663: an anonymous researcher

<https://support.apple.com/en-us/HT212336>

How bad is it? Remember Solarwinds Hack?

- Attackers used a system path.
 - On smartphones, we cannot (legitimately) access system paths.
- A VBScript, typically named after existing services or folders to blend into legitimate activities on the machine
 - A second-stage DLL implant, a custom Cobalt Strike loader, typically compiled uniquely per machine and written into a legitimate-looking subfolder in *%WinDir%* (e.g., `C:\Windows`)

How bad is it? In-ability to extract payloads

<https://googleprojectzero.blogspot.com/2019/08/implant-teardown.html>

In the earlier posts we examined how the attackers gained unsandboxed code execution as root on iPhones. At the end of each chain we saw the attackers calling `posix_spawn`, passing the path to their implant binary which they dropped in `/tmp`. This starts the implant running in the background as root. There is no visual indicator on the device that the implant is running. There's no way for a user on iOS to view a process listing, so the implant binary makes no attempt to hide its execution from the system.

IOC: “`/tmp/68753A44-4D6F-1226-9C60-0050E4C00067`”

This folder is blocked due to sandbox restrictions.

How bad is it? In-ability to extract payloads

- Some of NSO's IOCs:
 - `/private/var/db/com.apple.xpc.roleaccountd.staging/rs`
 - `/private/var/tmp/uevkjdwxiyah/c`
- These folders are blocked due to sandbox restrictions

Food for thought

- Missing / “confusing” mentioning. Why?
- Security Updates for Unsupported Devices == used in the wild?
- Why are we still blocked from extracting payloads / analyzing memory?
- Where are the IOCs?

Disadvantages of using LPE

- Problematic to share / disclose = keeping a potential weakness
- Unstable
- Porting
- Can be patched / new mitigation can prevent access for a while
- Race against attackers: time bomb is activated as soon as the discovery begins
- Using at scale
- It's unreasonable to request every SOC/analyst to have LPE 0days

Time bomb

NSO-Pegasus.pdf

Self-Destruct Mechanism

The Pegasus system contains **self-destruct mechanism** for the installed agents. In general, we understand that it is more important that the source will not be exposed and the target will suspect nothing than keeping the agent alive and working. The mechanism is activated in the following scenarios:

- **Risk of exposure:** In cases where a **great probability of exposing the agent exists**, a self-destruct mechanism is automatically being activated and the agent is uninstalled. Agent can be once again installed at a later time.
- **Agent is not responding:** In cases where the agent is not responding and **did not communicate with the servers for a long times**, the agent will automatically uninstall itself to prevent being exposed or misused.

Source: Pegasus / NSO Product Guide leak

BUT BUT BUT: Common Myths Dissected



BUSTED!

The “Walled Garden” has an Open Gate

- Walled garden is not really applicable to attackers.
- Attackers leverage 0 clicks or 1 clicks to infect targets.
- Let’s see what NSO has to say about the “Walled Garden”

Myth: “Walled Garden”

BUSTED!

Remote Installation (range free):

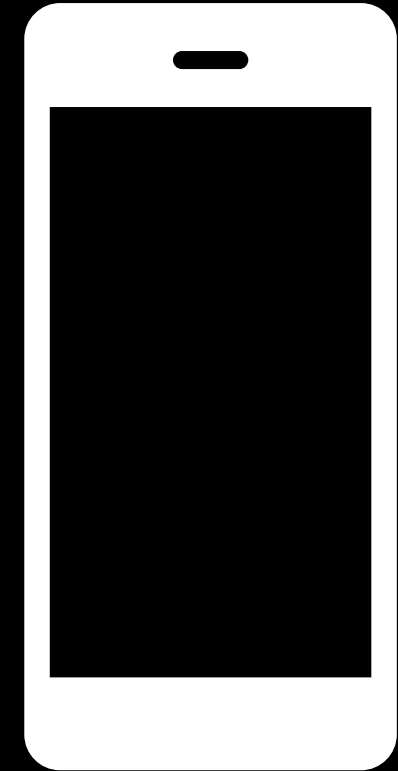
- **Over-the-Air (OTA):** A push message is remotely and covertly sent to the mobile device. This message triggers the device to download and install the agent on the device. During the entire installation process no cooperation or engagement of the target is required (e.g., clicking a link, opening a message) and no indication appears on the device. The installation is totally silent and invisible and cannot be prevented by the target. This is NSO uniqueness, which significantly differentiates the Pegasus solution from any other solution available in the market.
- **Enhanced Social Engineering Message (ESEM):** In cases where OTA installation method is inapplicable¹, the system operator can choose to send a regular text message (SMS) or an email, luring the target to open it. Single click, either planned or unintentional, on the link will result in hidden agent installation. The installation is entirely concealed and although the target clicked the link they will not be aware that software is being installed on their device.

Attackers like NSO leverage 0 clicks or 1 clicks to infect targets, not the app-store.

BUSTED!

Security Research Devices (SRD)

- Common myth: SRD helps analysis. In reality: it can only help to find vulnerabilities
- It does **NOT** help to analyze/extract payloads from production devices
- SRD? => Checkm8



BUSTED!

User should not be allowed to run elevated code?



Root access On
macOS = Okay
iOS = Not okay.
Why?

macOS Is No Less Secure Than iOS

Ron Okamoto

Vice President, Developer Relations



Q. Have you ever heard anybody at Apple say that the macOS is a less secure platform than iOS?

A. **No, I haven't.**

Okamoto Dep. Tr. at 279:7-9



User should not be allowed to run elevated code?



Root access On macOS = Okay
iOS = Not okay.
Why?

Safety of Macs/macOS “In Their Own Words”

Because of this, Apple provides layers of protection to ensure that apps are free of known malware and haven't been tampered with. Additional protections enforce that access from apps to user data is carefully mediated. **These security controls provide a stable, secure platform for apps** enabling thousands of developers to deliver hundreds of thousands of apps for iOS, iPadOS, and macOS—**all without impacting system integrity.** And users can access these apps on their Apple devices without undue fear of viruses, malware, or unauthorized attacks.

PX-0461

Download apps safely from the Mac App Store. And the internet.

Now apps from both the App Store and the internet can be installed **worry-free.** App Review makes sure each app in

PX-0741

We design Mac hardware and software with advanced technologies that work together **to run apps more securely,** protect your data, and help keep you **safe on the web.** And with macOS Big Sur available as a free upgrade, it's easy to get the

PX0741



Ron Okamoto
VP, Developer Relations

- Q. Okay. And Apple doesn't think its unsafe to use a Mac, does it?
- A. **No. We don't think it's unsafe** to use a Mac.

Okamoto Dep. Tr. at 273:15-18

- Q. Okay. So it's fair to say that using a Mac is not insecure, right?
- A. Yes, I believe so.

Okamoto Dep. Tr. at 274:2-4



From EPIC Games vs. Apple Trial (2021)



BUSTED!

User should not be allowed to run elevated code?




Root access On
macOS = Okay
iOS = Not okay.
Why?



Additional MacOS Security Mechanisms Are Replicable on iOS



Craig Federighi
Apple Senior Vice President of Software Engineering



Q. You could **implement** all the mechanisms that are current -- **all the layers that are currently in macOS** [on iOS]; correct?

A. **Yes.**

Federighi Dep. Tr. at 80:2-5

Feature	macOS 	iOS 
Malware Removal Tool (MRT)	✓	replicable
XProtect	✓	replicable
Notarization	✓	replicable
Gatekeeper	✓	replicable

From EPIC Games vs. Apple Trial (2021)



BUSTED!

User is not allowed to run elevated code



Tunnel Traffic (VPN)



Profiles



Root Certificate



Wipe Device (MDM)



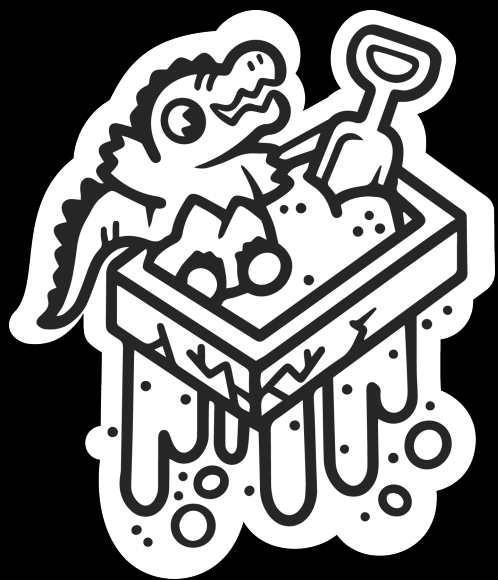
Root access (macOS)



Validate Own Device

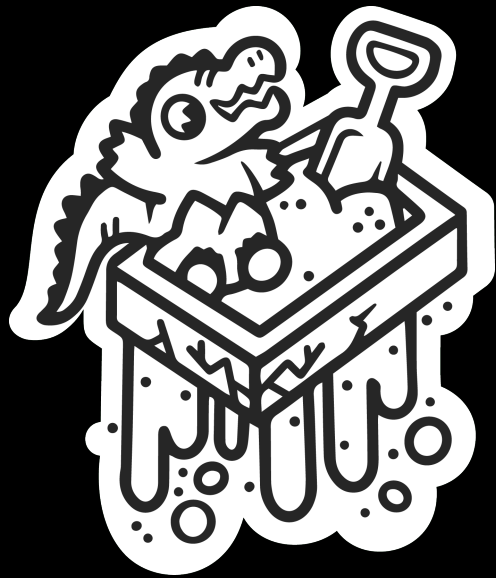


What is #FreeTheSandbox?



- A non-profit initiative to promote open-sandbox policy for device-owners.
- Local admin user w/ flexible sandbox policy enables independent attestation, payloads extraction to prevent further misuse, and even innovation!

#FreeTheSandbox Security Goals

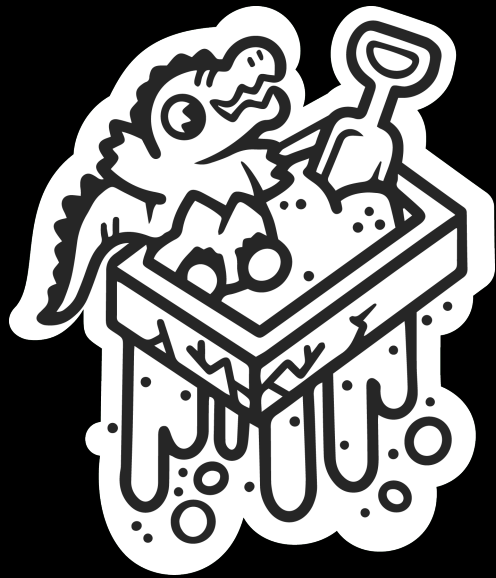


Creation of an administrator / root level user

RO Access to entire filesystem for persistent attacks

RO Access to memory for non-persistent attacks

#FreeTheSandbox Global Goals



Enable additional innovation using these amazing devices.

E.g. VMWare, various types of authentication, etc.

What Can We Do?

Convince vendors opening the sandbox is net positive

- Safer platform — More attacks will get discovered
- \$\$\$\$ — Win more CYOD contracts
- Innovation

What Can We Do? Policy-Makers

Mobile are becoming a significant risk.
It's time to adapt the law.



Thank You

Get in-touch



zuk.av@zecops.com



[@ihackbanme](https://twitter.com/ihackbanme)

