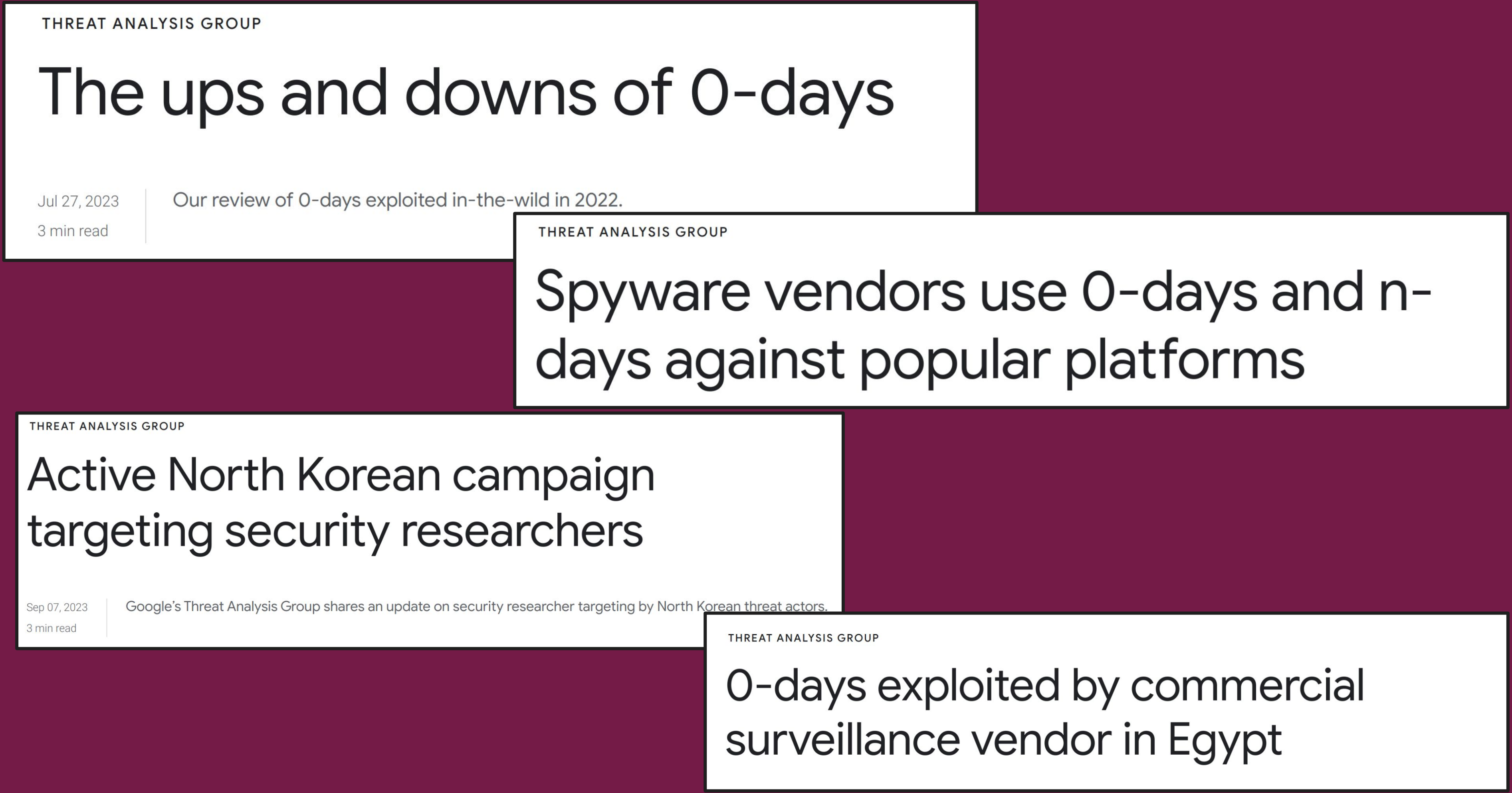
When Exploits Aren’t Binary

Maddie Stone
@maddiestone

BSides Canberra 2023

Hi, I’m Maddie 👋

and exploits are my favorite



THREAT ANALYSIS GROUP

The ups and downs of 0-days

Jul 27, 2023
3 min read

Our review of 0-days exploited in-the-wild in 2022.

THREAT ANALYSIS GROUP

Spyware vendors use 0-days and n-days against popular platforms

THREAT ANALYSIS GROUP

Active North Korean campaign targeting security researchers

Sep 07, 2023
3 min read

Google's Threat Analysis Group shares an update on security researcher targeting by North Korean threat actors.

THREAT ANALYSIS GROUP

0-days exploited by commercial surveillance vendor in Egypt

CVE-2023-0266 - Android Kernel

CVE-2023-26083 - Android Mali GPU

CVE-2023-21492 - Samsung

CVE-2023-28205 - Safari

CVE-2023-28206 - iOS

CVE-2023-2033 - Chrome

CVE-2023-2136 - Chrome

CVE-2023-32409 - Safari

CVE-2023-3079 - Chrome

CVE-2023-37580 - Zimbra

CVE-2023-36874 - Windows

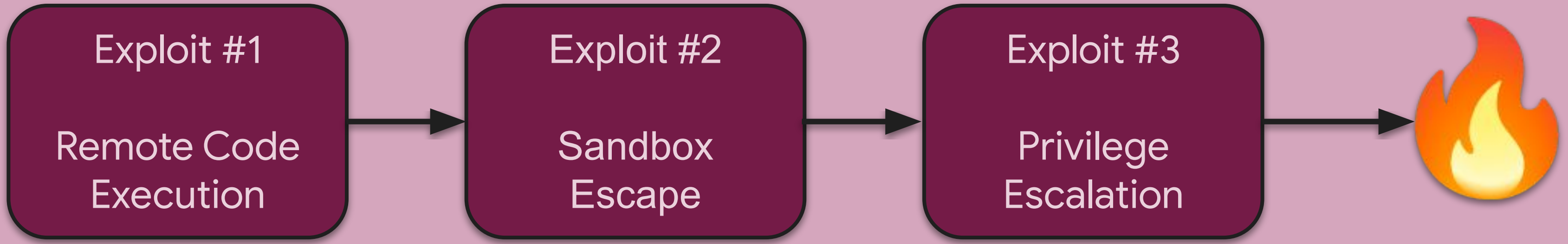
CVE-2023-36884 - Microsoft Office/IE

CVE-2023-41993 - Safari

CVE-2023-41991 - iOS

CVE-2023-41992 - iOS

CVE-2023-5217 - Chrome



Exploit #1

Remote Code Execution

Exploit #2

Sandbox Escape

Exploit #3

Privilege Escalation

🔥

Attackers will only do what is necessary to accomplish their goal.

Make them hack you with 0-days.

While 0-days may make up a small minority of attacks, each 0-day has an **outsized impact on society.**

0-day exploitation affects all of us even when we’re not the one being targeted.

Detect, analyze, and prevent 0-day* exploitation.

targeted
government backed
limited
sophisticated

0-day or n-day?

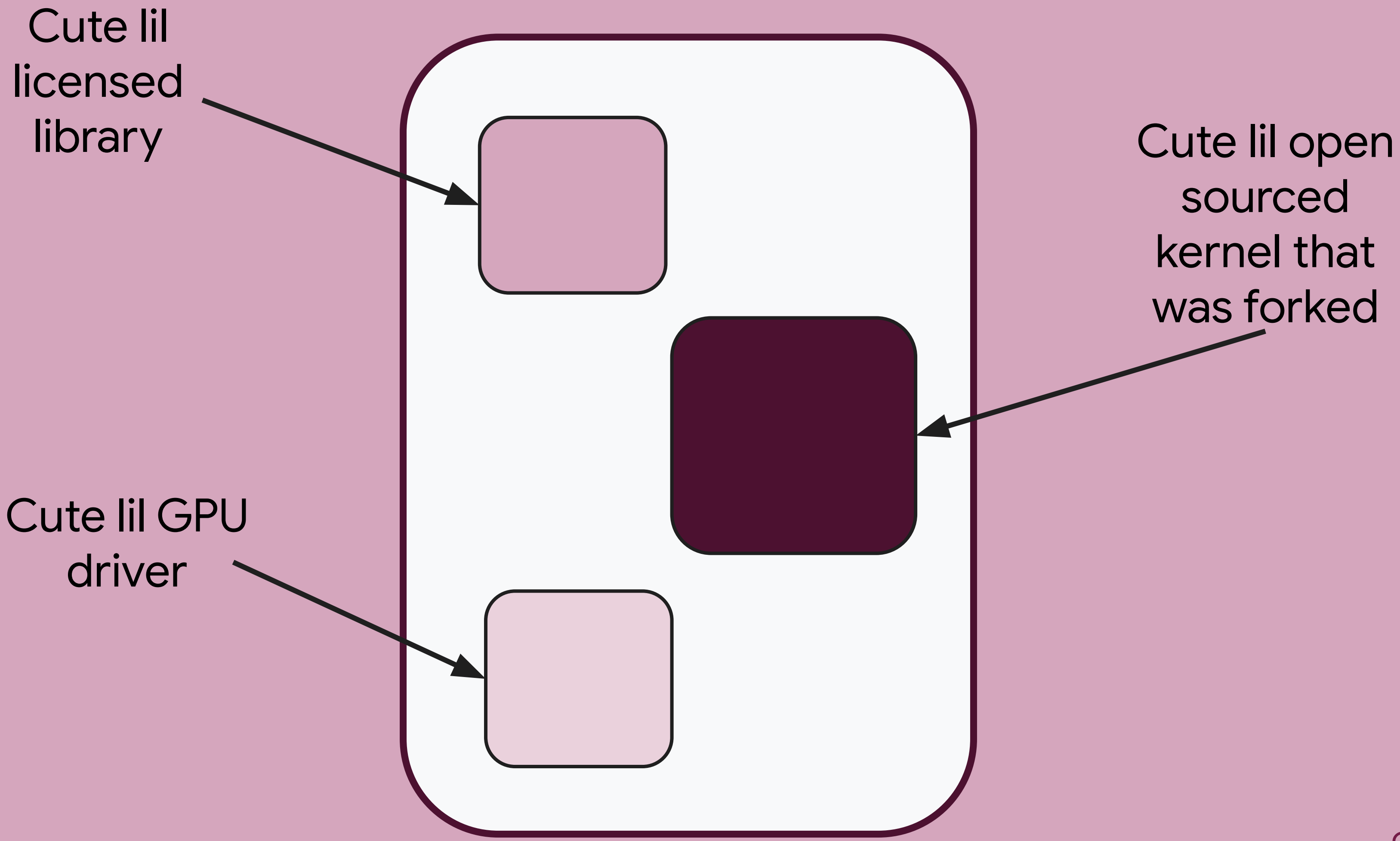
0-day: a vulnerability defenders **don’t** yet know about n-day: a vulnerability defenders **do** know about

or…

0-day: a vulnerability that doesn’t have a patch available

Where’s the confusion?

Cute lil product I’ve purchased that I expect to receive security updates to keep me protected



Cute lil licensed library

Cute lil open sourced kernel that was forked

Cute lil GPU driver

↑ Upstream releases a fix

↓ Downstream doesn’t release the fix

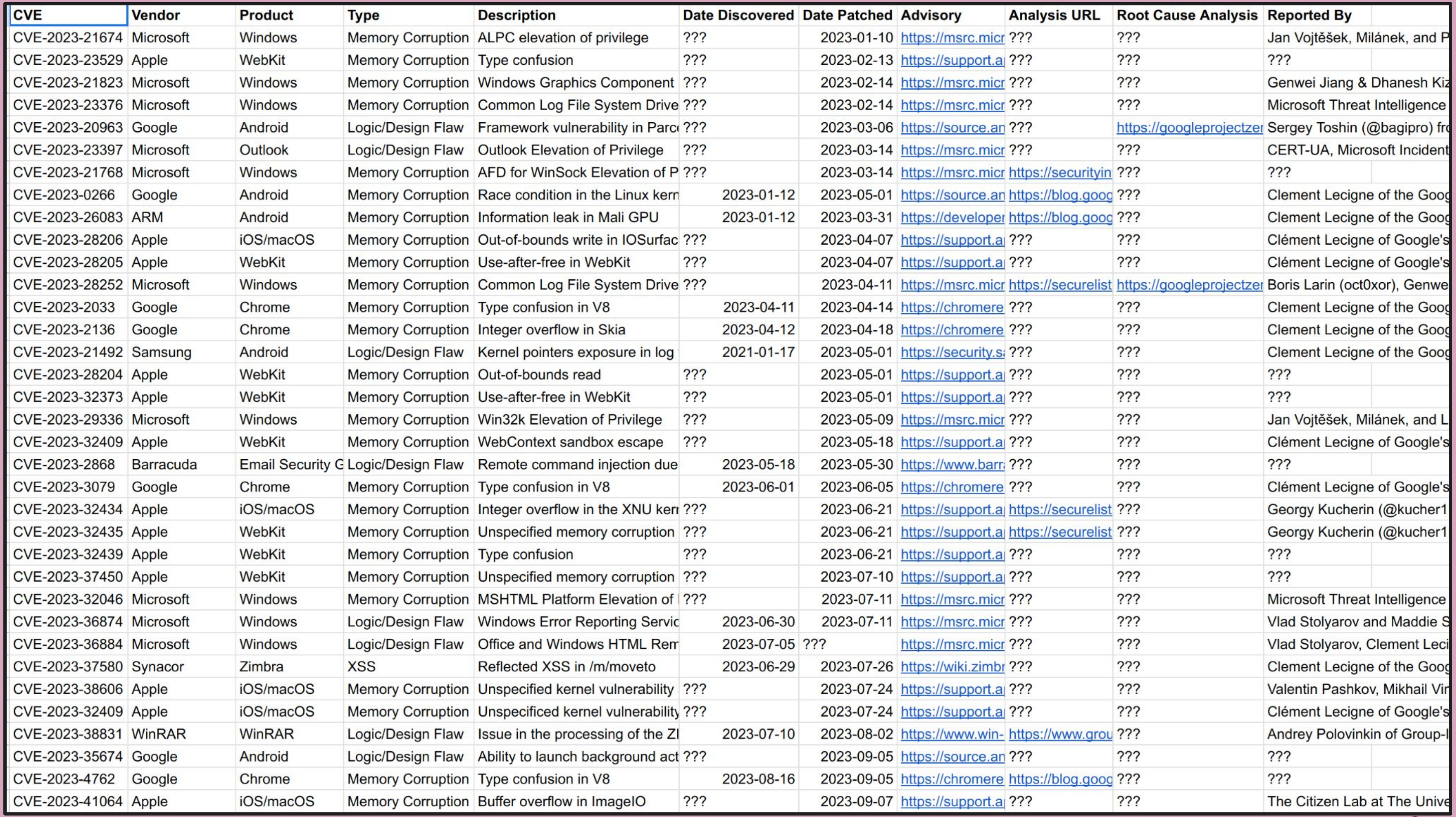
- A bug fixed upstream without a security advisory or CVE
- A product that doesn’t or hasn’t ever received security updates
- A bug that has been fully disclosed, but not patched
- A mitigation bypass

What are you trying to communicate?

Are you trying to communicate that…

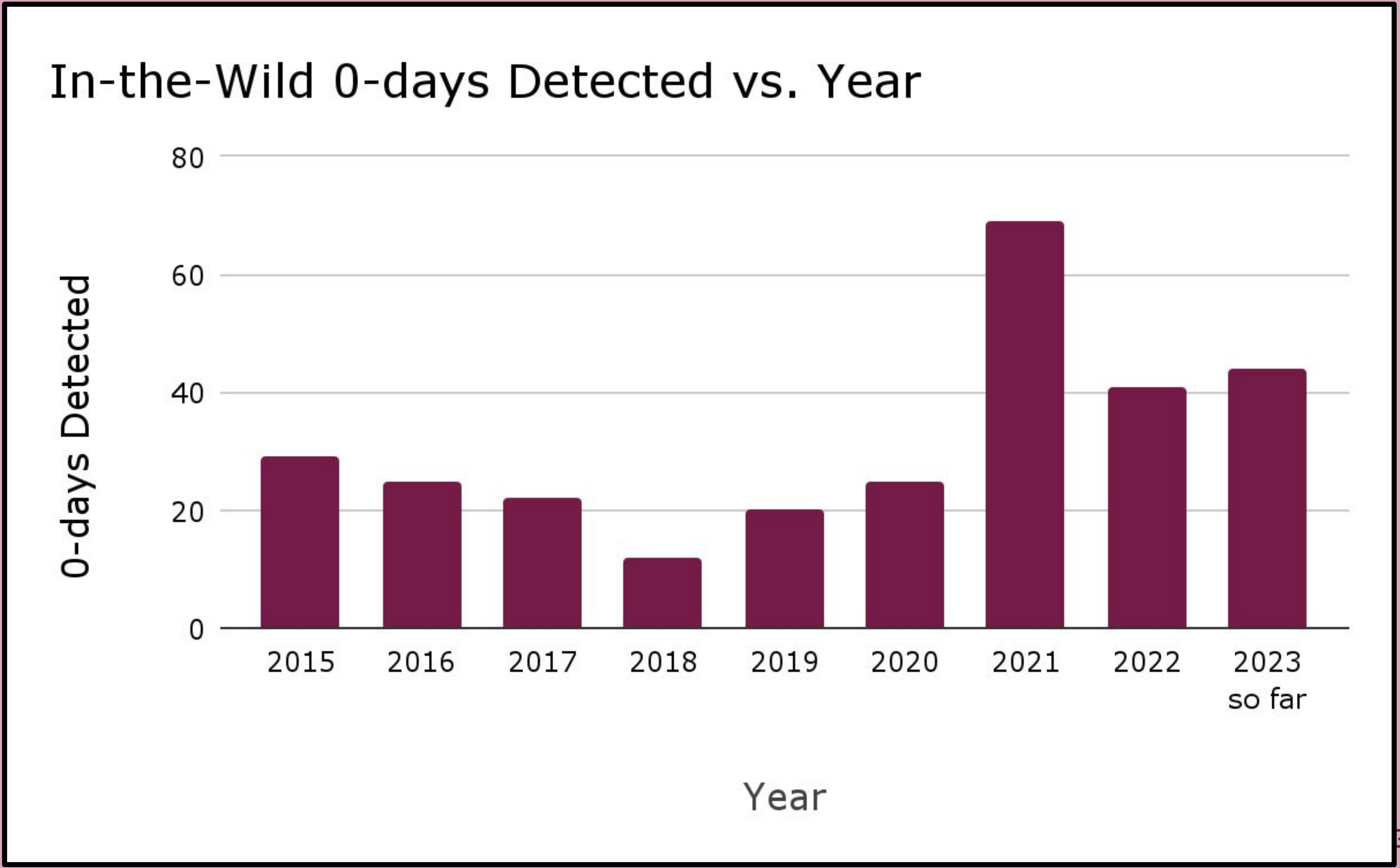
- Users don’t have a clear recourse to protect themselves
- The attack required significant expertise and resources
- There should be urgency
- It’s a bug defenders didn’t know exists

“N-days that function like 0-days”

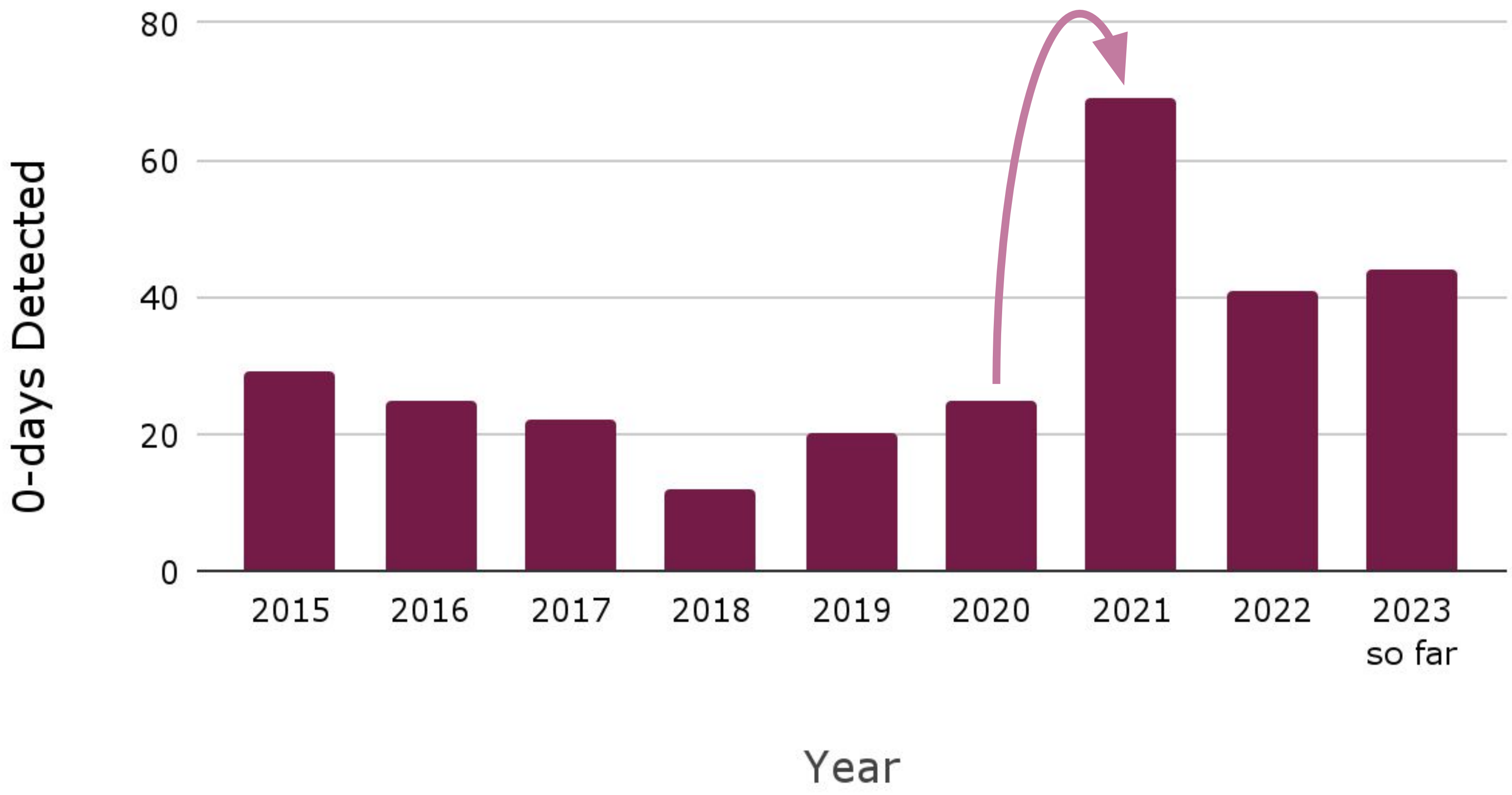


CVE	Vendor	Product	Type	Description	Date Discovered	Date Patched	Advisory	Analysis URL	Root Cause Analysis	Reported By
CVE-2023-21674	Microsoft	Windows	Memory Corruption	ALPC elevation of privilege	???	2023-01-10	https://msrc.micr	???	???	Jan Vojtěšek, Milánek, and P
CVE-2023-23529	Apple	WebKit	Memory Corruption	Type confusion	???	2023-02-13	https://support.a	???	???	???
CVE-2023-21823	Microsoft	Windows	Memory Corruption	Windows Graphics Component	???	2023-02-14	https://msrc.micr	???	???	Genwei Jiang & Dhanesh Kiz
CVE-2023-23376	Microsoft	Windows	Memory Corruption	Common Log File System Drive	???	2023-02-14	https://msrc.micr	???	???	Microsoft Threat Intelligence
CVE-2023-20963	Google	Android	Logic/Design Flaw	Framework vulnerability in Parc	???	2023-03-06	https://source.an	???	https://googleprojectzer	Sergey Toshin (@bagipro) fr
CVE-2023-23397	Microsoft	Outlook	Logic/Design Flaw	Outlook Elevation of Privilege	???	2023-03-14	https://msrc.micr	???	???	CERT-UA, Microsoft Incident
CVE-2023-21768	Microsoft	Windows	Memory Corruption	AFD for WinSock Elevation of P	???	2023-03-14	https://msrc.micr	https://securityin	???	???
CVE-2023-0266	Google	Android	Memory Corruption	Race condition in the Linux kern	2023-01-12	2023-05-01	https://source.an	https://blog.goog	???	Clement Lecigne of the Goog
CVE-2023-26083	ARM	Android	Memory Corruption	Information leak in Mali GPU	2023-01-12	2023-03-31	https://developer	https://blog.goog	???	Clement Lecigne of the Goog
CVE-2023-28206	Apple	iOS/macOS	Memory Corruption	Out-of-bounds write in IOSurfac	???	2023-04-07	https://support.a	???	???	Clément Lecigne of Google's
CVE-2023-28205	Apple	WebKit	Memory Corruption	Use-after-free in WebKit	???	2023-04-07	https://support.a	???	???	Clément Lecigne of Google's
CVE-2023-28252	Microsoft	Windows	Memory Corruption	Common Log File System Drive	???	2023-04-11	https://msrc.micr	https://securelist	https://googleprojectzer	Boris Larin (oct0xor), Genwe
CVE-2023-2033	Google	Chrome	Memory Corruption	Type confusion in V8	2023-04-11	2023-04-14	https://chromere	???	???	Clement Lecigne of the Goog
CVE-2023-2136	Google	Chrome	Memory Corruption	Integer overflow in Skia	2023-04-12	2023-04-18	https://chromere	???	???	Clement Lecigne of the Goog
CVE-2023-21492	Samsung	Android	Logic/Design Flaw	Kernel pointers exposure in log	2021-01-17	2023-05-01	https://security.s	???	???	Clement Lecigne of the Goog
CVE-2023-28204	Apple	WebKit	Memory Corruption	Out-of-bounds read	???	2023-05-01	https://support.a	???	???	???
CVE-2023-32373	Apple	WebKit	Memory Corruption	Use-after-free in WebKit	???	2023-05-01	https://support.a	???	???	???
CVE-2023-29336	Microsoft	Windows	Memory Corruption	Win32k Elevation of Privilege	???	2023-05-09	https://msrc.micr	???	???	Jan Vojtěšek, Milánek, and L
CVE-2023-32409	Apple	WebKit	Memory Corruption	WebContext sandbox escape	???	2023-05-18	https://support.a	???	???	Clément Lecigne of Google's
CVE-2023-2868	Barracuda	Email Security G	Logic/Design Flaw	Remote command injection due	2023-05-18	2023-05-30	https://www.barr	???	???	???
CVE-2023-3079	Google	Chrome	Memory Corruption	Type confusion in V8	2023-06-01	2023-06-05	https://chromere	???	???	Clément Lecigne of Google's
CVE-2023-32434	Apple	iOS/macOS	Memory Corruption	Integer overflow in the XNU kerr	???	2023-06-21	https://support.a	https://securelist	???	Georgy Kucherin (@kucher1
CVE-2023-32435	Apple	WebKit	Memory Corruption	Unspecified memory corruption	???	2023-06-21	https://support.a	https://securelist	???	Georgy Kucherin (@kucher1
CVE-2023-32439	Apple	WebKit	Memory Corruption	Type confusion	???	2023-06-21	https://support.a	???	???	???
CVE-2023-37450	Apple	WebKit	Memory Corruption	Unspecified memory corruption	???	2023-07-10	https://support.a	???	???	???
CVE-2023-32046	Microsoft	Windows	Memory Corruption	MSHTML Platform Elevation of	???	2023-07-11	https://msrc.micr	???	???	Microsoft Threat Intelligence
CVE-2023-36874	Microsoft	Windows	Logic/Design Flaw	Windows Error Reporting Servic	2023-06-30	2023-07-11	https://msrc.micr	???	???	Vlad Stolyarov and Maddie S
CVE-2023-36884	Microsoft	Windows	Logic/Design Flaw	Office and Windows HTML Rem	2023-07-05	???	https://msrc.micr	???	???	Vlad Stolyarov, Clement Leci
CVE-2023-37580	Synacor	Zimbra	XSS	Reflected XSS in /m/moveto	2023-06-29	2023-07-26	https://wiki.zimbr	???	???	Clement Lecigne of the Goog
CVE-2023-38606	Apple	iOS/macOS	Memory Corruption	Unspecified kernel vulnerability	???	2023-07-24	https://support.a	???	???	Valentin Pashkov, Mikhail Vir
CVE-2023-32409	Apple	iOS/macOS	Memory Corruption	Unspecificed kernel vulnerability	???	2023-07-24	https://support.a	???	???	Clément Lecigne of Google's
CVE-2023-38831	WinRAR	WinRAR	Logic/Design Flaw	Issue in the processing of the ZI	2023-07-10	2023-08-02	https://www.win-	https://www.grou	???	Andrey Polovinkin of Group-I
CVE-2023-35674	Google	Android	Logic/Design Flaw	Ability to launch background act	???	2023-09-05	https://source.an	???	???	???
CVE-2023-4762	Google	Chrome	Memory Corruption	Type confusion in V8	2023-08-16	2023-09-05	https://chromere	https://blog.goog	???	???
CVE-2023-41064	Apple	iOS/macOS	Memory Corruption	Buffer overflow in ImageIO	???	2023-09-07	https://support.a	???	???	The Citizen Lab at The Unive

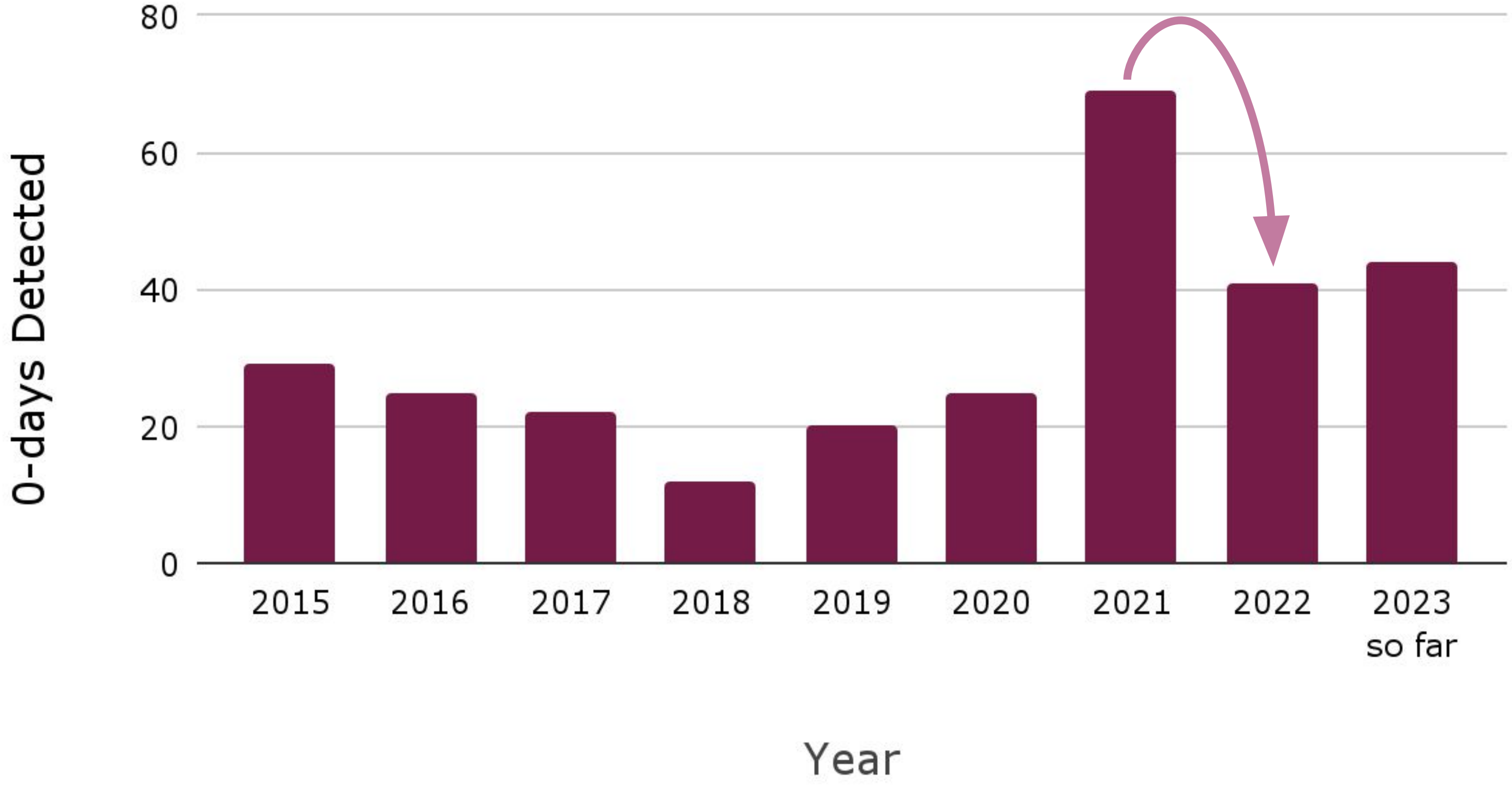
https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY


In-the-Wild 0-days Detected vs. Year
0-days Detected
80
60
40
20
0
2015
2016
2017
2018
2019
2020
2021
2022
2023 so far
Year

In-the-Wild 0-days Detected vs. Year



In-the-Wild 0-days Detected vs. Year



What does the number of in-the-wild 0-days mean? 🤔

detected & disclosed

What does the number of in-the-wild 0-days mean? 🤔

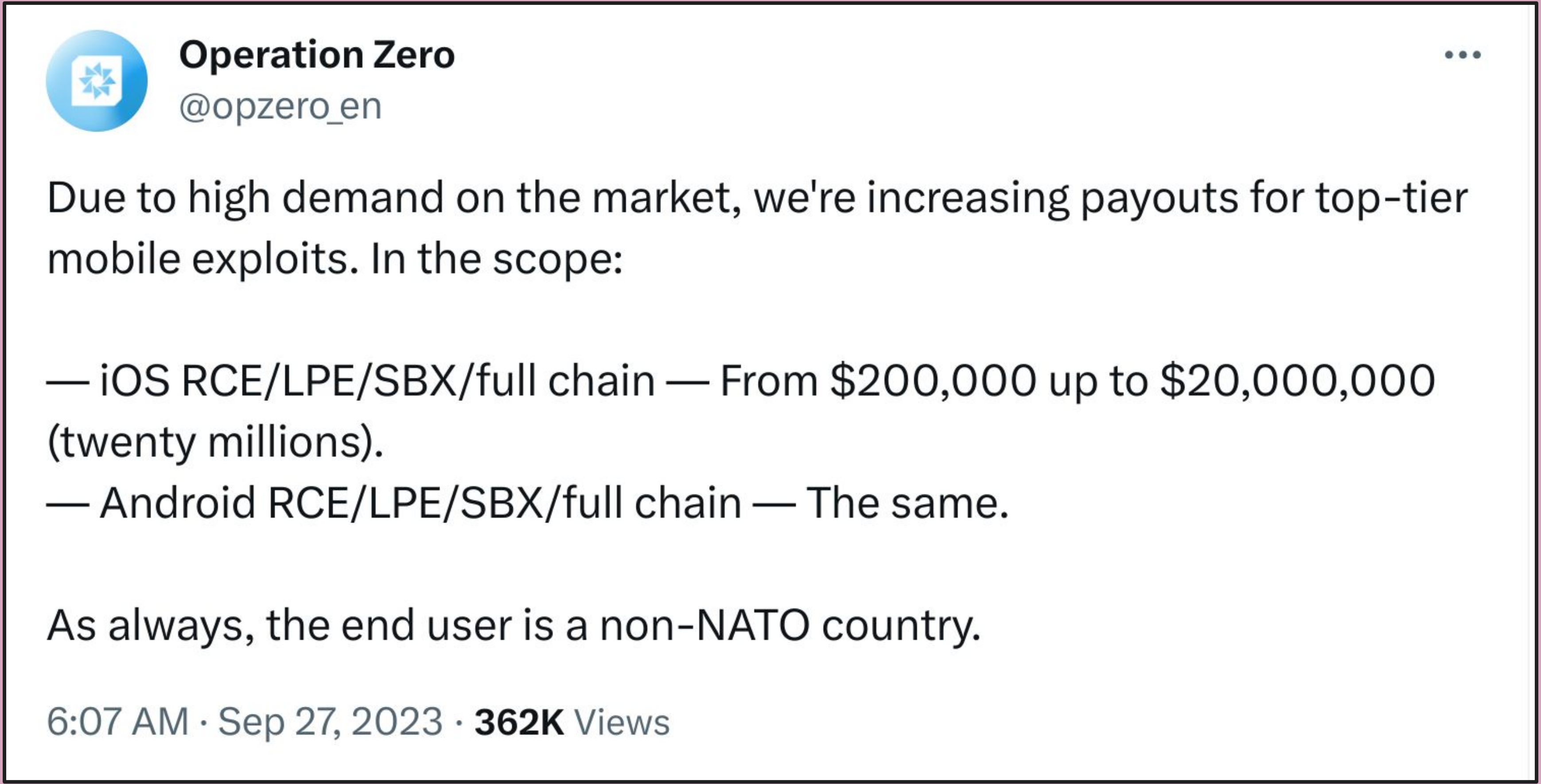
The number of 0-days detected and disclosed in-the-wild can’t tell us much about the state of security.

“Make 0day hard.”

- Google Project Zero’s Mission

1. Increase cost* per 0-day

✨ TANGENT ✨



Operation Zero
@opzero_en

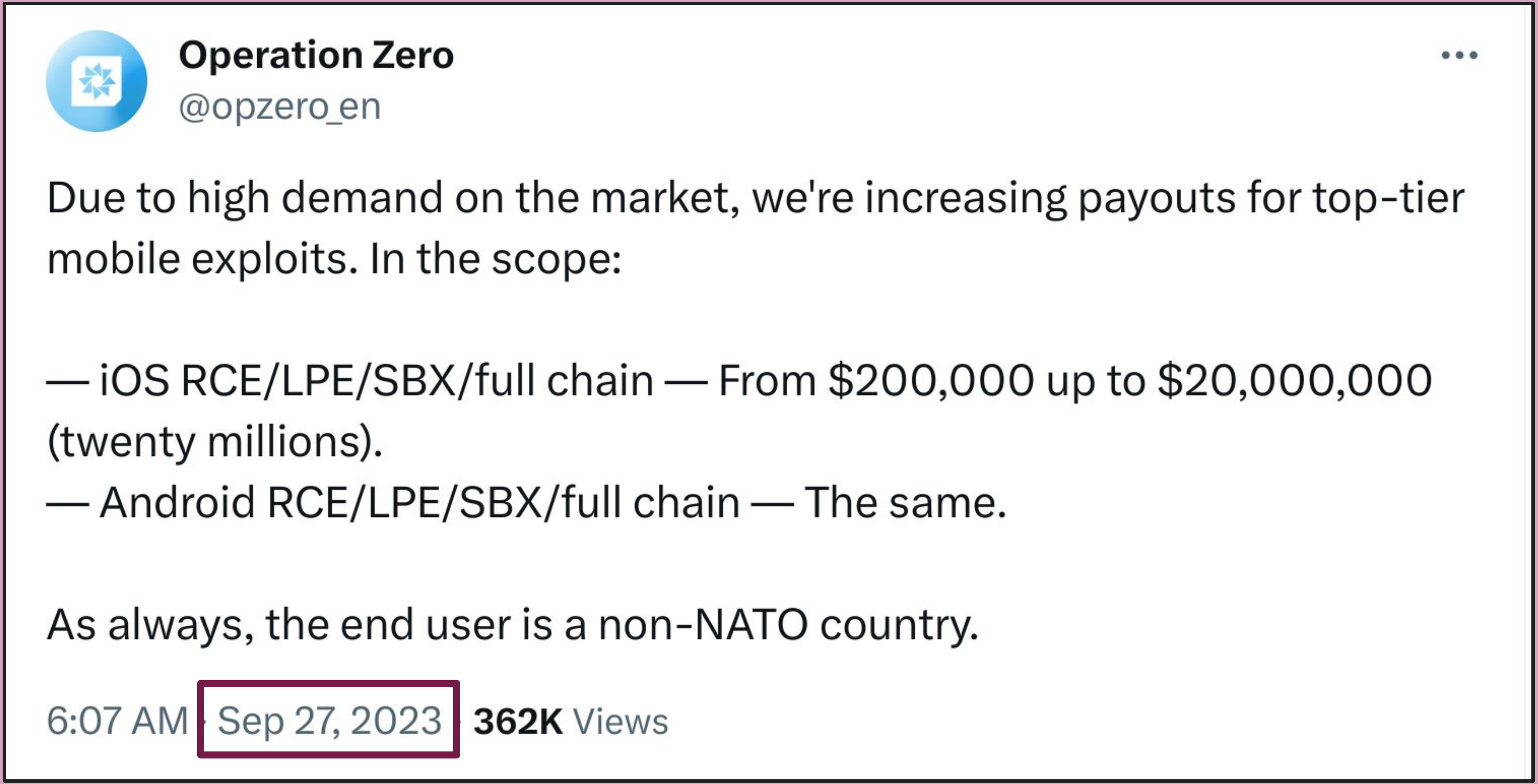
Due to high demand on the market, we're increasing payouts for top-tier mobile exploits. In the scope:

— iOS RCE/LPE/SBX/full chain — From $200,000 up to $20,000,000 (twenty millions).
— Android RCE/LPE/SBX/full chain — The same.

As always, the end user is a non-NATO country.

6:07 AM · Sep 27, 2023 · **362K** Views

https://twitter.com/opzero_en/status/1706762507631677760



Operation Zero
@opzero_en

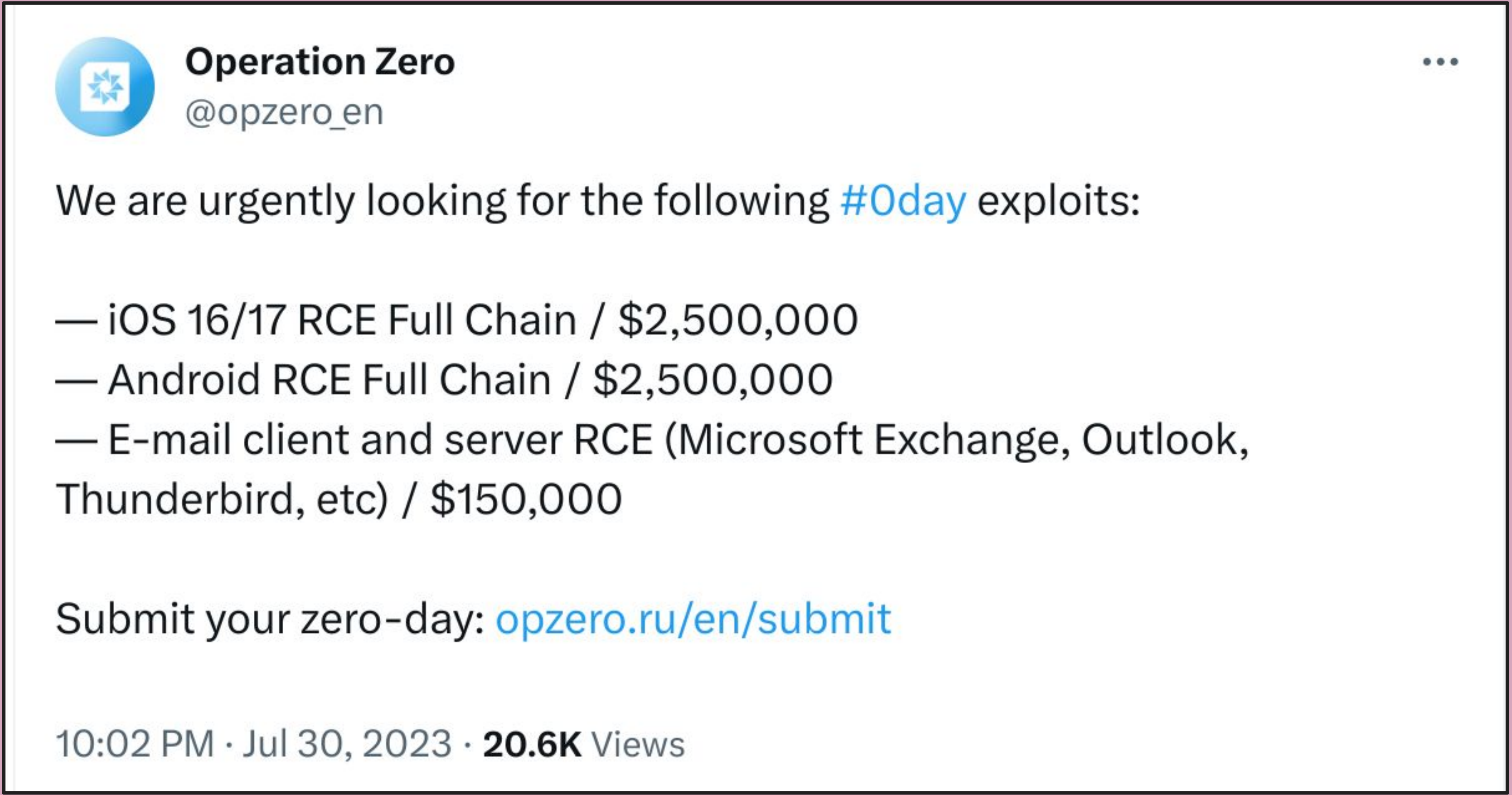
Due to high demand on the market, we're increasing payouts for top-tier mobile exploits. In the scope:

— iOS RCE/LPE/SBX/full chain — From $200,000 up to $20,000,000 (twenty millions).
— Android RCE/LPE/SBX/full chain — The same.

As always, the end user is a non-NATO country.

6:07 AM · Sep 27, 2023 · **362K** Views

https://twitter.com/opzero_en/status/1706762507631677760



Operation Zero
@opzero_en

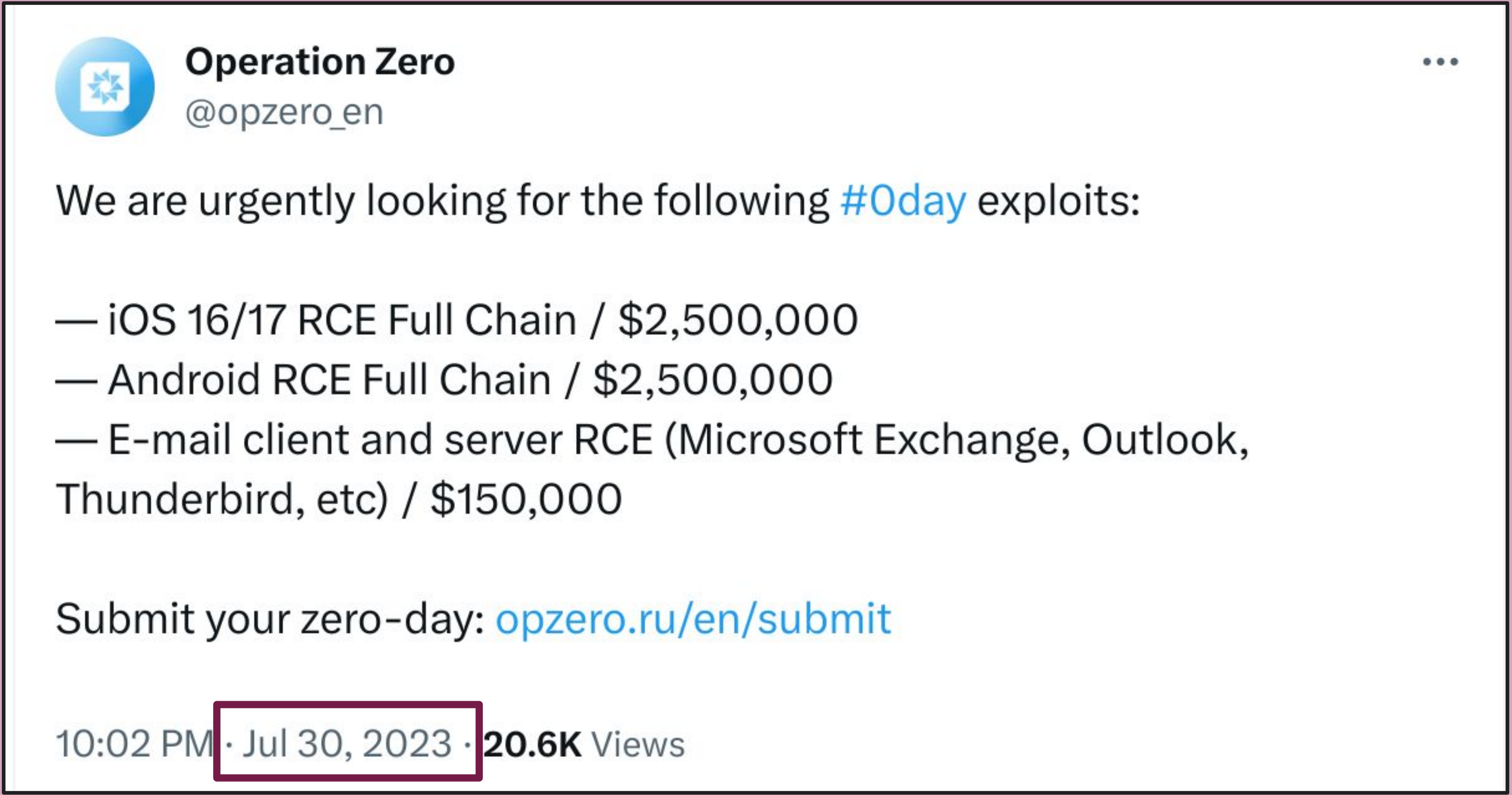
We are urgently looking for the following #0day exploits:

— iOS 16/17 RCE Full Chain / $2,500,000
— Android RCE Full Chain / $2,500,000
— E-mail client and server RCE (Microsoft Exchange, Outlook, Thunderbird, etc) / $150,000

Submit your zero-day: opzero.ru/en/submit

10:02 PM · Jul 30, 2023 · **20.6K** Views

https://twitter.com/opzero_en/status/1685621799311048705



Operation Zero
@opzero_en

We are urgently looking for the following #0day exploits:

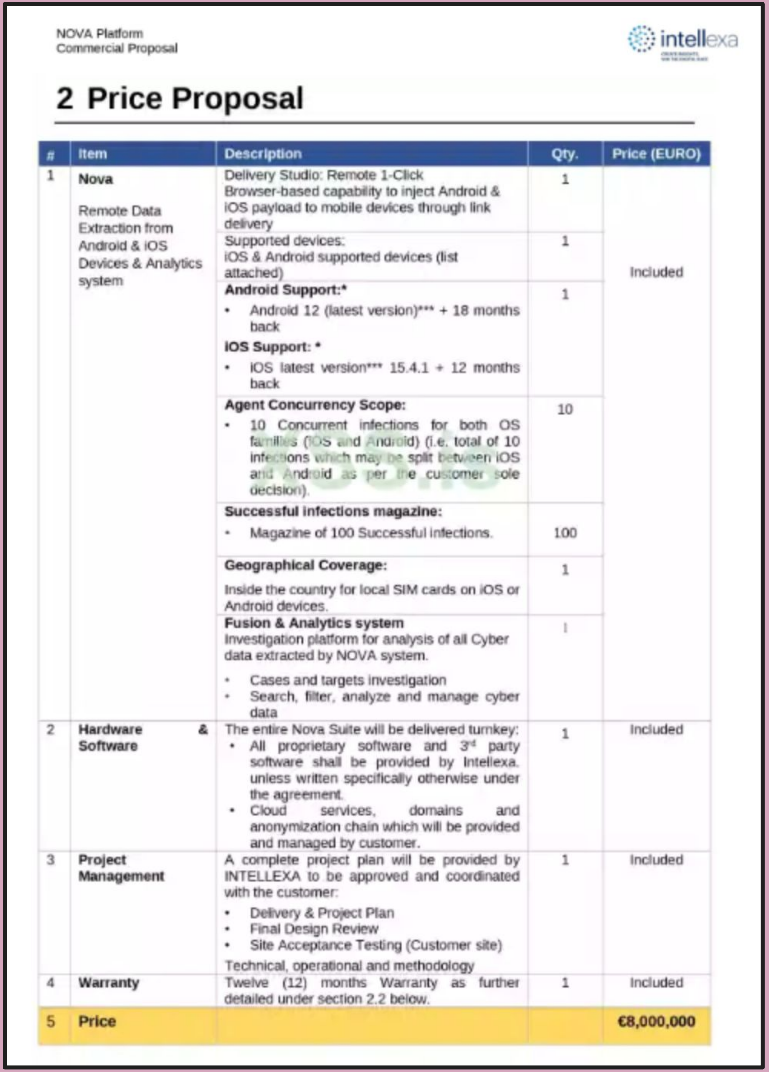
— iOS 16/17 RCE Full Chain / $2,500,000
— Android RCE Full Chain / $2,500,000
— E-mail client and server RCE (Microsoft Exchange, Outlook, Thunderbird, etc) / $150,000

Submit your zero-day: opzero.ru/en/submit

10:02 PM · Jul 30, 2023 · **20.6K** Views

https://twitter.com/opzero_en/status/1685621799311048705

Intellexa leak
August 2022

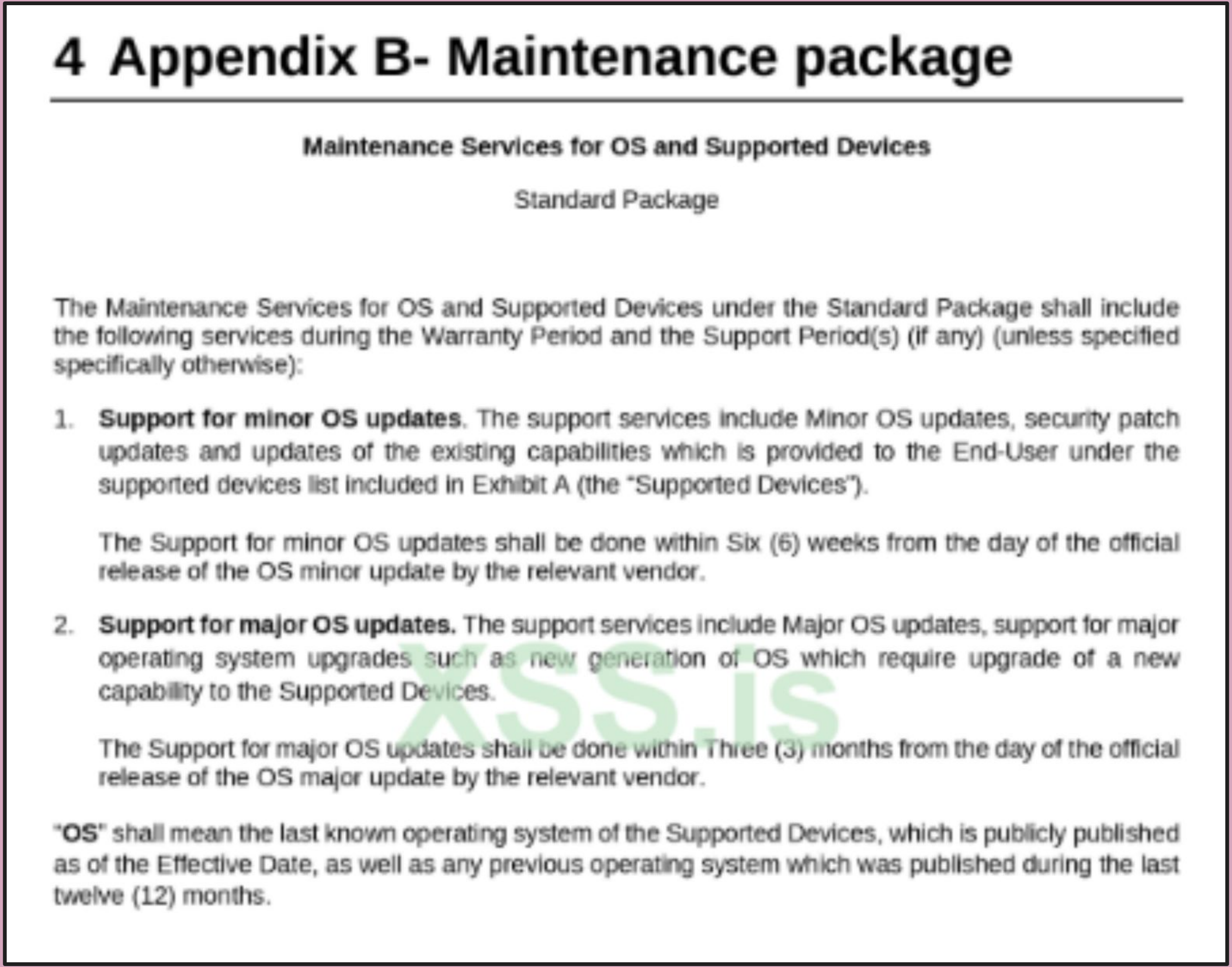


NOVA Platform
Commercial Proposal

2 Price Proposal

#	Item	Description	Qty.	Price (EURO)
1	**Nova** Remote Data Extraction from Android & iOS Devices & Analytics system	Delivery Studio: Remote 1-Click Browser-based capability to inject Android & iOS payload to mobile devices through link delivery	1	Included
		Supported devices: iOS & Android supported devices (list attached)	1	
		Android Support:* • Android 12 (latest version)*** + 18 months back **iOS Support: *** • iOS latest version*** 15.4.1 + 12 months back	1	
		Agent Concurrency Scope: • 10 Concurrent infections for both OS families (iOS and Android) (i.e. total of 10 infections which may be split between iOS and Android as per the customer sole decision).	10	
		Successful infections magazine: • Magazine of 100 Successful infections.	100	
		Geographical Coverage: Inside the country for local SIM cards on iOS or Android devices.	1	
		Fusion & Analytics system Investigation platform for analysis of all Cyber data extracted by NOVA system. • Cases and targets investigation • Search, filter, analyze and manage cyber data	1	
2	**Hardware & Software**	The entire Nova Suite will be delivered turnkey: • All proprietary software and 3rd party software shall be provided by Intellexa. unless written specifically otherwise under the agreement. • Cloud services, domains and anonymization chain which will be provided and managed by customer.	1	Included
3	**Project Management**	A complete project plan will be provided by INTELLEXA to be approved and coordinated with the customer: • Delivery & Project Plan • Final Design Review • Site Acceptance Testing (Customer site) Technical, operational and methodology	1	Included
4	**Warranty**	Twelve (12) months Warranty as further detailed under section 2.2 below.	1	Included
5	**Price**			**€8,000,000**

€8,000,000



4 Appendix B- Maintenance package

Maintenance Services for OS and Supported Devices

Standard Package

The Maintenance Services for OS and Supported Devices under the Standard Package shall include the following services during the Warranty Period and the Support Period(s) (if any) (unless specified specifically otherwise):

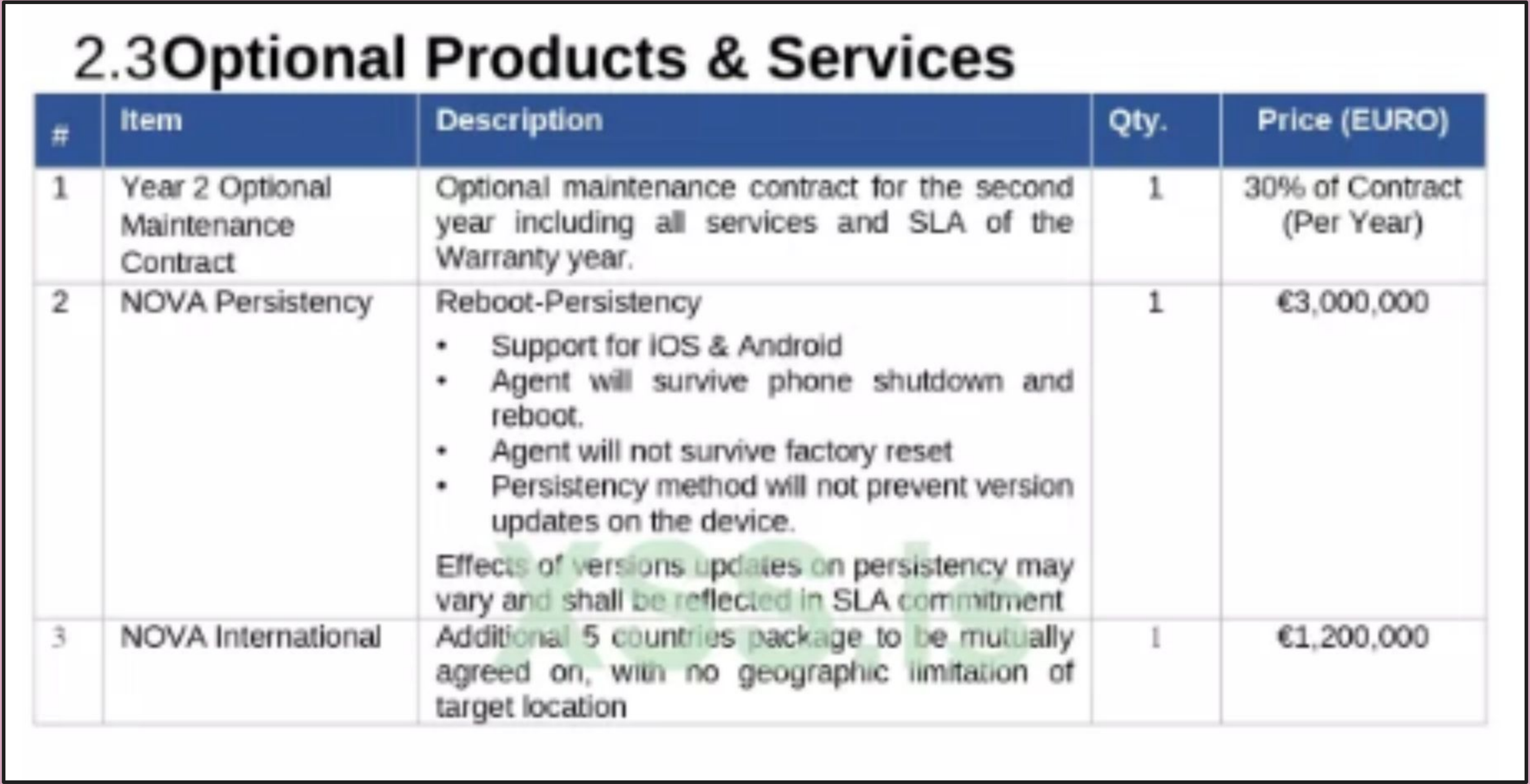
1. **Support for minor OS updates**. The support services include Minor OS updates, security patch updates and updates of the existing capabilities which is provided to the End-User under the supported devices list included in Exhibit A (the "Supported Devices").

   The Support for minor OS updates shall be done within Six (6) weeks from the day of the official release of the OS minor update by the relevant vendor.

2. **Support for major OS updates.** The support services include Major OS updates, support for major operating system upgrades such as new generation of OS which require upgrade of a new capability to the Supported Devices.

   The Support for major OS updates shall be done within Three (3) months from the day of the official release of the OS major update by the relevant vendor.

"**OS**" shall mean the last known operating system of the Supported Devices, which is publicly published as of the Effective Date, as well as any previous operating system which was published during the last twelve (12) months.



2.3Optional Products & Services

#	Item	Description	Qty.	Price (EURO)
1	Year 2 Optional Maintenance Contract	Optional maintenance contract for the second year including all services and SLA of the Warranty year.	1	30% of Contract (Per Year)
2	NOVA Persistency	Reboot-Persistency • Support for iOS & Android • Agent will survive phone shutdown and reboot. • Agent will not survive factory reset • Persistency method will not prevent version updates on the device. Effects of versions updates on persistency may vary and shall be reflected in SLA commitment	1	€3,000,000
3	NOVA International	Additional 5 countries package to be mutually agreed on, with no geographic limitation of target location	1	€1,200,000

1. Increase cost* per 0-day

Cost to develop a 0-day

!=

Cost to buy a 0-day

1. Increase cost* per 0-day

*time, money, expertise

1. Increase cost* per 0-day

*time, money, expertise

2. Increase number of 0-days required

1. Increase cost* per 0-day

*time, money, expertise

2. Increase number of 0-days required

Costs more for a less useful 0-day.

What does the number of in-the-wild 0-days mean? 🤔

Causes Number to Go **Up**

- More folks disclosing when a 0-day is known to be in-the-wild 🎉
- Discovering & fixing 0-days more quickly 🎉
- Adding security boundaries to platforms 🎉

Causes Number to Go **Down**

Causes Number to Go **Up**

- Discovering & fixing 0-days more quickly 🎉
- More folks disclosing when a 0-day is known to be in-the-wild 🎉
- Adding security boundaries to platforms 🎉
- Variant analysis is not performed on reported vulnerabilities 😢
- Exploit techniques are not mitigated 😢
- More exploitable vulnerabilities are added to code than fixed 😢

Causes Number to Go **Down**

Causes Number to Go **Up**

- Discovering & fixing 0-days more quickly 🎉
- More folks disclosing when a 0-day is known to be in-the-wild 🎉
- Adding security boundaries to platforms 🎉
- Variant analysis is not performed on reported vulnerabilities 😢
- Exploit techniques are not mitigated 😢
- More exploitable vulnerabilities are added to code than fixed 😢

Causes Number to Go **Down**

- Fewer exploitable 0-day vulnerabilities exist 🎉
- Each new 0-day requires the creation of a new exploitation technique 🎉
- New vulnerabilities require researching new attack surfaces 🎉

Causes Number to Go **Up**

- Discovering & fixing 0-days more quickly 🎉
- More folks disclosing when a 0-day is known to be in-the-wild 🎉
- Adding security boundaries to platforms 🎉
- Variant analysis is not performed on reported vulnerabilities 😢
- Exploit techniques are not mitigated 😢
- More exploitable vulnerabilities are added to code than fixed 😢

Causes Number to Go **Down**

- Fewer exploitable 0-day vulnerabilities exist 🎉
- Each new 0-day requires the creation of a new exploitation technique 🎉
- New vulnerabilities require researching new attack surfaces 🎉
- Slower to detect in-the-wild 0-days so a bug has a longer lifetime 😢
- Longer until users are able to install a patch 😢
- Less sophisticated attack methods are sufficient 😢

From the 2022 Year in Review Report:

N-days function like 0-days on Android due to long patching times. Across the Android ecosystem there were multiple cases where patches were not available to users for a significant time. Attackers didn't need 0-day exploits and instead were able to use n-days that functioned as 0-days.

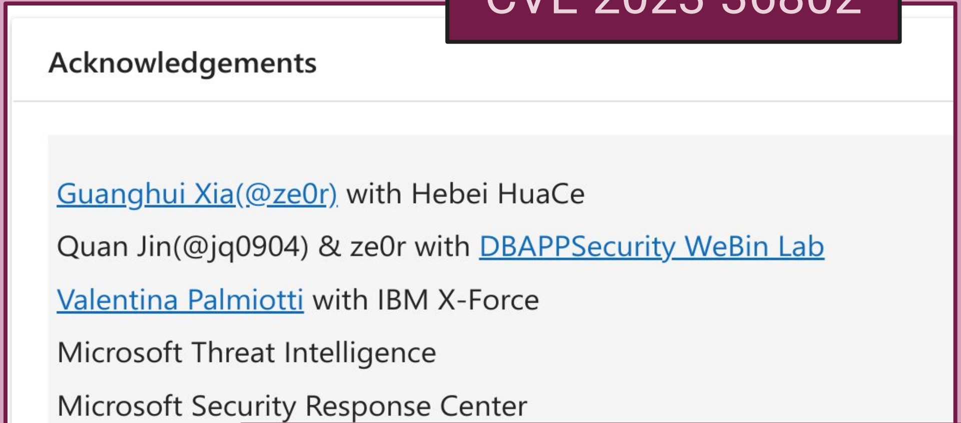
0-click exploits and new browser mitigations drive down browser 0-days. Many attackers have been moving towards 0-click rather than 1-click exploits. 0-clicks usually target components other than the browser. In addition, all major browsers also implemented new defenses that make exploiting a vulnerability more difficult and could have influenced attackers moving to other attack surfaces.

Over 40% of the 0-days discovered were variants of previously reported vulnerabilities. Seventeen out of the 41 in-the-wild 0-days from 2022 are variants of previously reported vulnerabilities. This continues the unpleasant trend that we've discussed previously in both the 2020 Year in Review report and the mid-way through 2022 report. More than 20% are variants of previous in-the-wild 0-days from 2021 and 2020.

Bug collisions are high. 2022 brought more frequent reports of attackers using the same vulnerabilities as each other, as well as security researchers reporting vulnerabilities that were later discovered to be used by attackers. When an in-the-wild 0-day targeting a popular consumer platform is found and fixed, it's increasingly likely to be breaking another attacker's exploit as well.

Bug Collisions

CVE-2023-36802



Acknowledgements

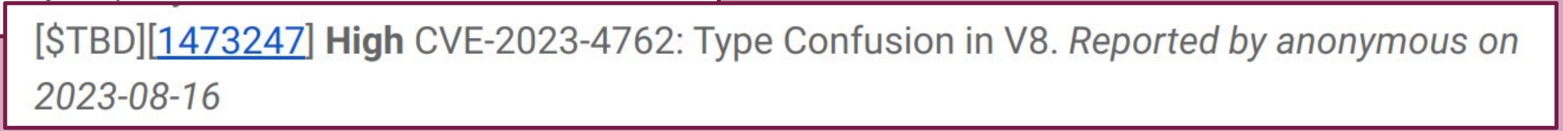
Guanghui Xia(@ze0r) with Hebei HuaCe

Quan Jin(@jq0904) & ze0r with DBAPPSecurity WeBin Lab

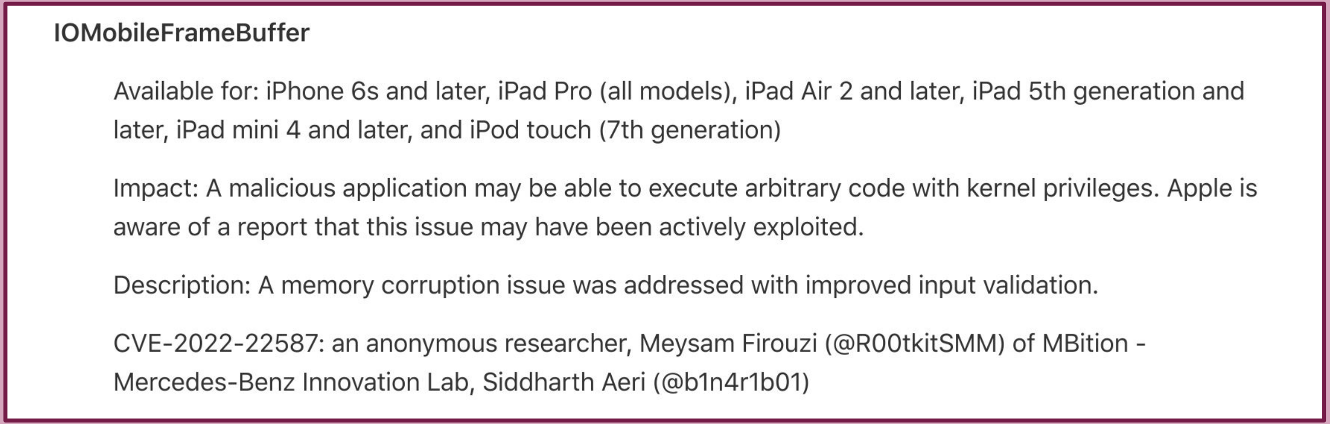
Valentina Palmiotti with IBM X-Force

Microsoft Threat Intelligence

Microsoft Security Response Center



[$TBD][1473247] **High** CVE-2023-4762: Type Confusion in V8. *Reported by anonymous on 2023-08-16*



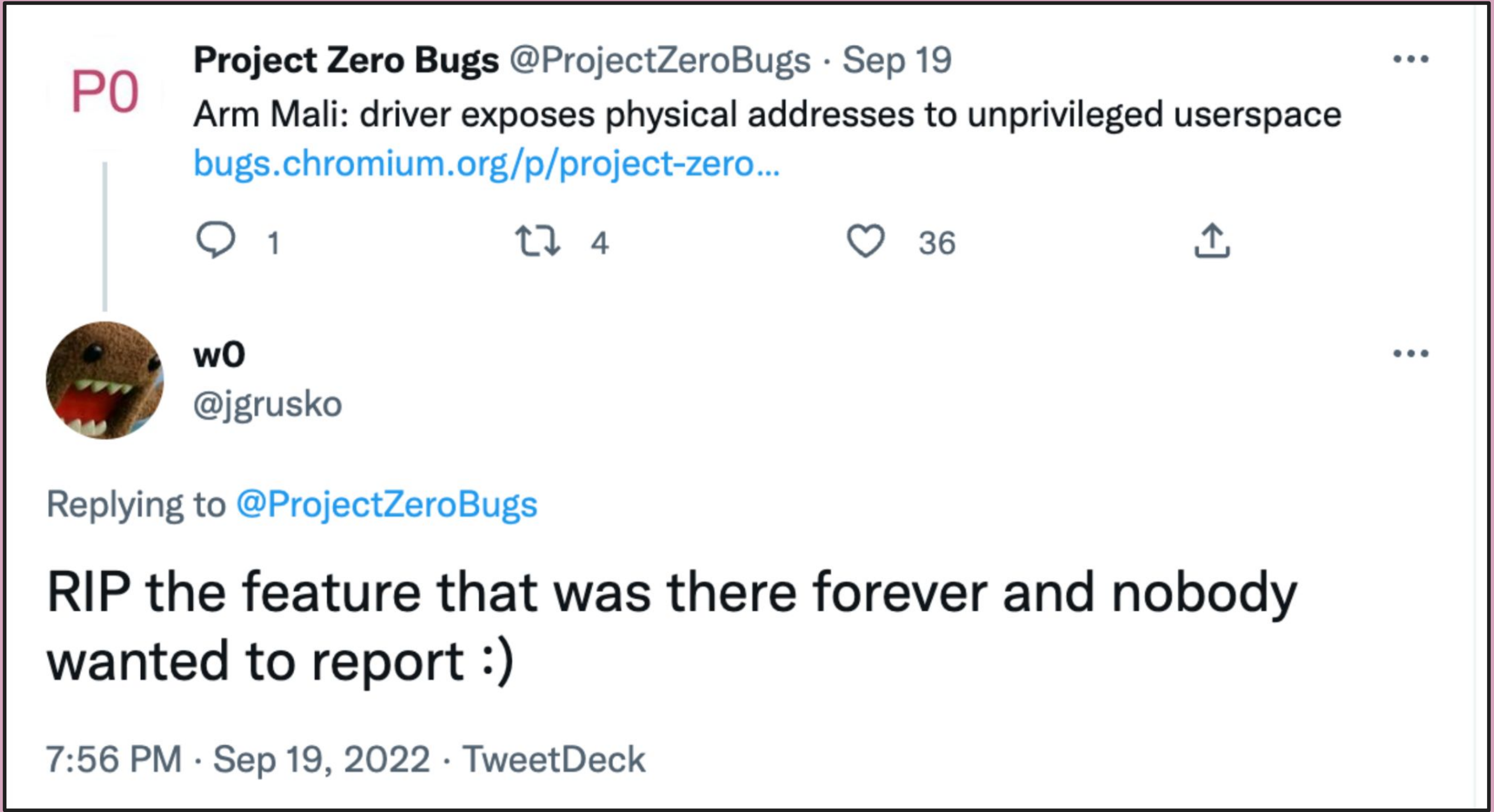
IOMobileFrameBuffer

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: A malicious application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.

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

CVE-2022-22587: an anonymous researcher, Meysam Firouzi (@R00tkitSMM) of MBition - Mercedes-Benz Innovation Lab, Siddharth Aeri (@b1n4r1b01)



Project Zero Bugs @ProjectZeroBugs · Sep 19

Arm Mali: driver exposes physical addresses to unprivileged userspace bugs.chromium.org/p/project-zero...

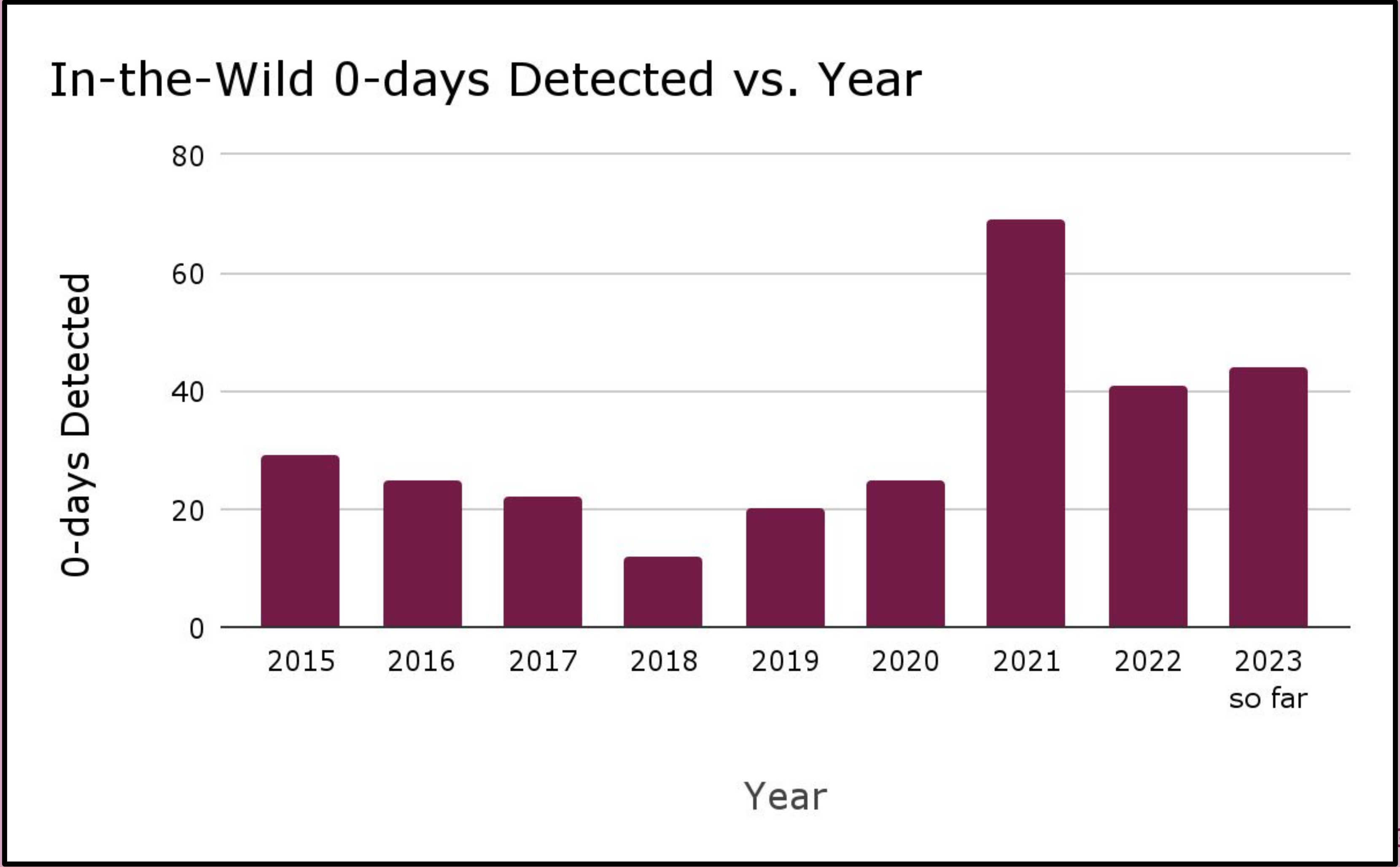
w0
@jgrusko

Replying to @ProjectZeroBugs

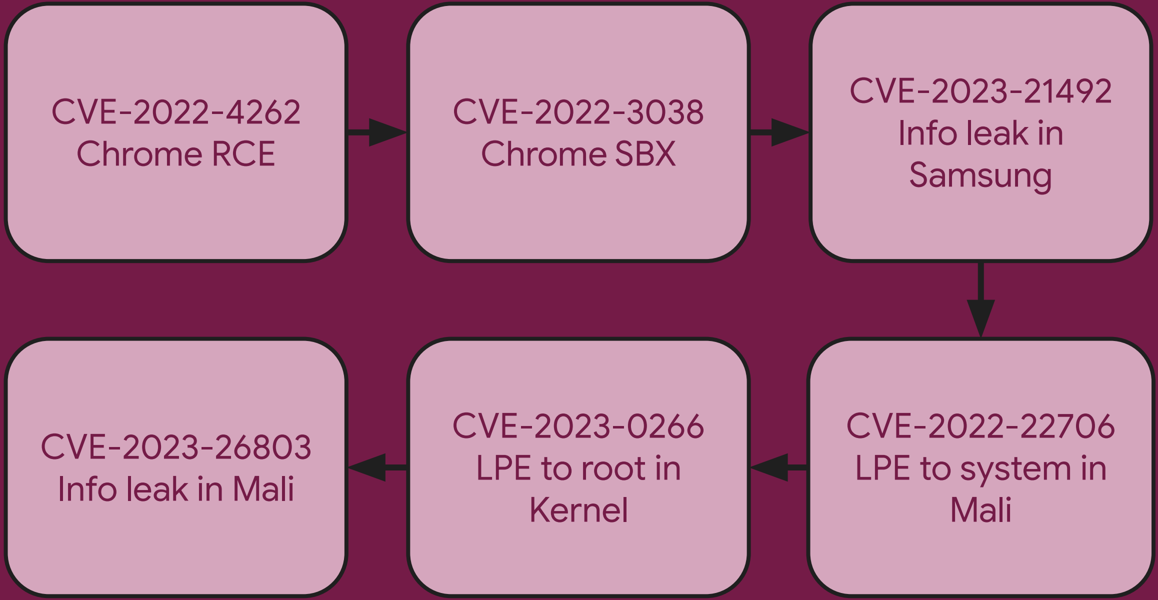
RIP the feature that was there forever and nobody wanted to report :)

7:56 PM · Sep 19, 2022 · TweetDeck

https://twitter.com/jgrusko/status/1571921203723440135


In-the-Wild 0-days Detected vs. Year
0-days Detected
80
60
40
20
0
2015
2016
2017
2018
2019
2020
2021
2022
2023 so far
Year

Dec 2022 Variston Campaign in UAE



CVE-2022-4262
Chrome RCE

CVE-2022-3038
Chrome SBX

CVE-2023-21492
Info leak in Samsung

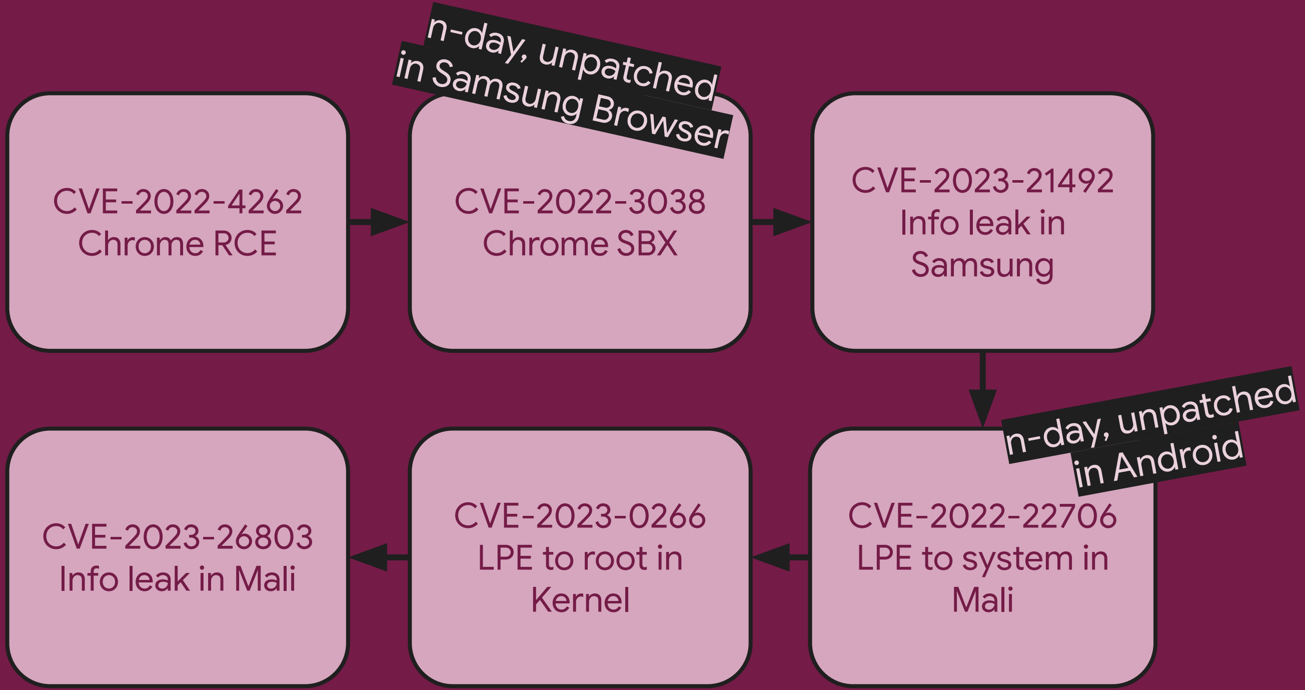
CVE-2022-22706
LPE to system in Mali

CVE-2023-0266
LPE to root in Kernel

CVE-2023-26803
Info leak in Mali

Google

Dec 2022 Variston Campaign in UAE



CVE-2022-4262
Chrome RCE

n-day, unpatched in Samsung Browser

CVE-2022-3038
Chrome SBX

CVE-2023-21492
Info leak in Samsung

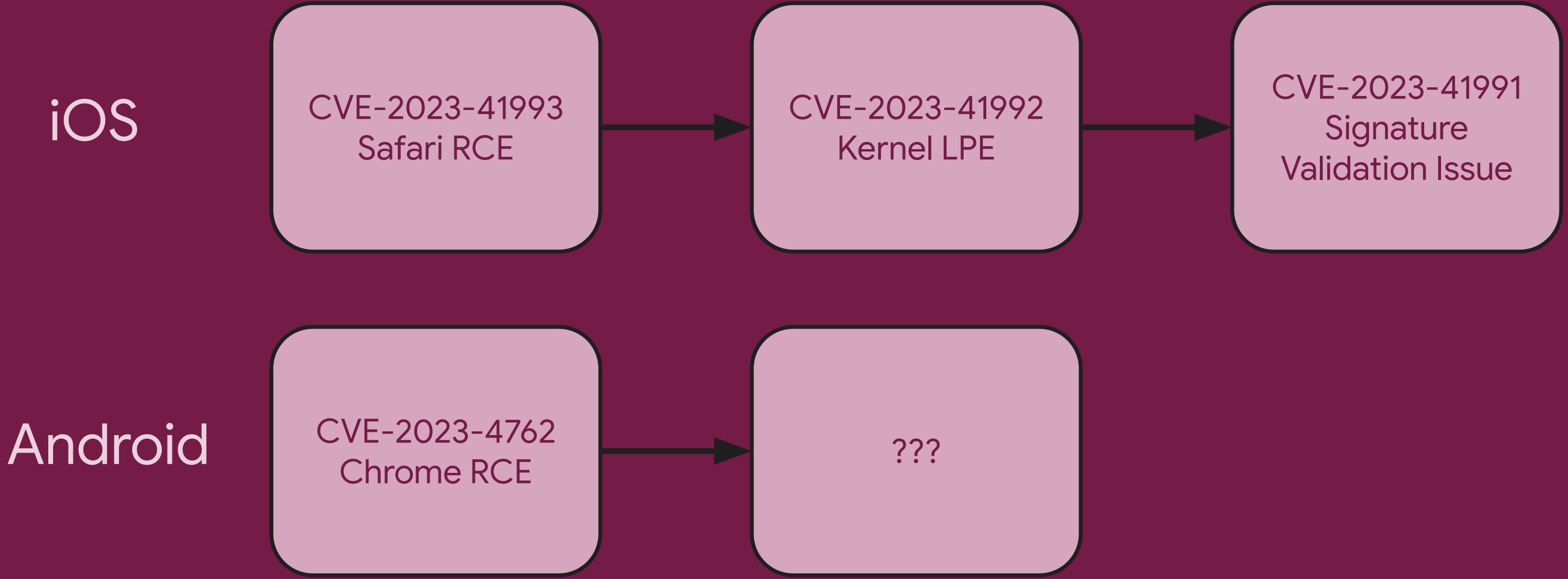
n-day, unpatched in Android

CVE-2022-22706
LPE to system in Mali

CVE-2023-0266
LPE to root in Kernel

CVE-2023-26803
Info leak in Mali

Sept 2023 Intellexa Campaign in Egypt



iOS

CVE-2023-41993
Safari RCE

CVE-2023-41992
Kernel LPE

CVE-2023-41991
Signature
Validation Issue

Android

CVE-2023-4762
Chrome RCE

???

What can we do?

There has been **significant progress** in security.

Don’t let perfection be the enemy of good.

Vendor response to reported vulnerabilities

- Get fixes and mitigations to users quickly so that they can protect themselves.
- Perform detailed analyses to ensure the root cause of the vulnerability is addressed.
- Share as many technical details as possible.
- Capitalize on reported vulnerabilities to learn and fix as much as we can from them.

Thank you!

@maddiestone

0day-in-the-wild <at> google <dot> com