n-1 and *n*-2:
Should we really trust in you?

(An examination of  macOS security updates)

Joshua Long

*with a few notes added to the slides for clarity

Objective by the Sea

intego

% whoami

Joshua Long

- Chief Security Analyst at Intego
- 20+ years of cyber threat research
- Master of IT in Internet Security
- Discovered Apple ID password validation vulnerability
- Twitter: @theJoshMeister

Objective by the Sea

intego

n-1 and *n*-2: Should we really trust in you?

- A brief history of macOS security updates
- Are new macOS versions inherently safer?
- Comparing patches for 400+ Big Sur-era vulns
- What about iOS?
- Takeaways

Objective by the Sea

intego

Security update 2003-11-19 for 10.2.8

“It is Apple's policy to quickly address significant vulnerabilities in past releases of Mac OS X wherever feasible.”

* To date, this remains one of very few public statements Apple has made regarding its security update policies.

2003 2012 2021

Objective by the Sea

intego

Security update 2003-11-19 for 10.2.8

“It is Apple's policy to quickly address significant vulnerabilities in past releases of Mac OS X wherever feasible.”

Security updates, 2003-12-19

“Note: The following fixes which appear in "Security Update 2003-12-19 for Panther" are not included in "Security Update 2003-12-19 for Jaguar" since the Jaguar versions of Mac OS X and Mac OS X Server are not vulnerable to these issues”

* Unfortunately, Apple no longer makes statements like these, which leaves open to speculation why some vulnerabilities don’t get patched for some macOS versions.

2003 2012 2021

Objective by the Sea

intego

n and *n*-1

* Eventually Apple started patching a few apps (such as iTunes, QuickTime, and Safari) for the "n-2" Mac OS X version as well.

2003 2012 2021

September 2012:
Apple solidifies “n-2” support

* … when they started releasing security updates simultaneously for Mac OS X versions 10.6, 10.7, and 10.8.

Apple has followed similar practices ever since then.

2003 **2012** **2021**

Objective by the Sea

intego

Why do Mac users sometimes not upgrade to the latest macOS?

- Don’t think they need the new features
- Concerned about something breaking
- Use legacy apps that won’t run on the latest OS
- Older Macs may not be compatible with the latest OS

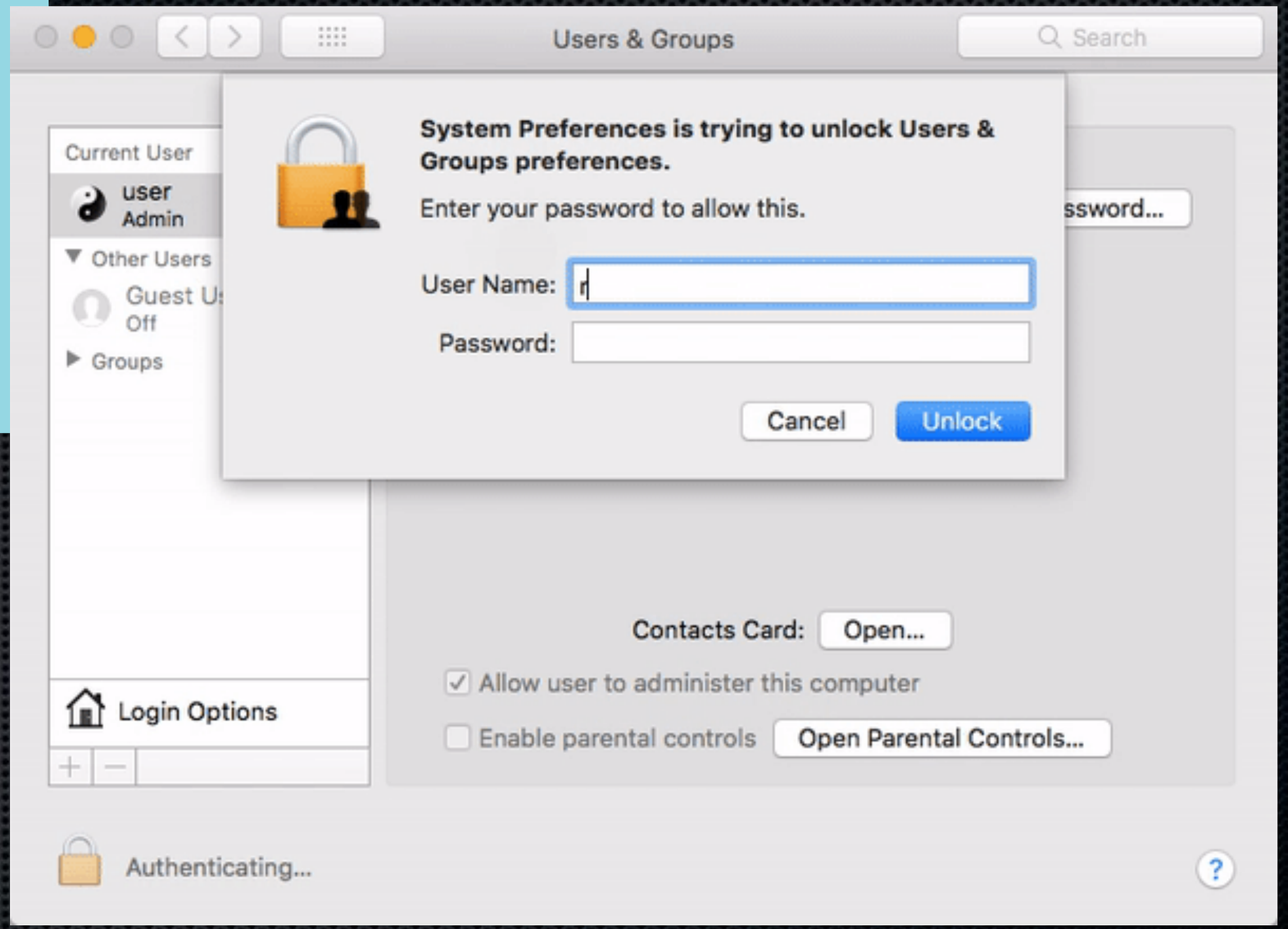
Myth #1: New macOS versions are inherently safer.

Nope.

Objective by the Sea

intego

Remember this?



macOS High Sierra

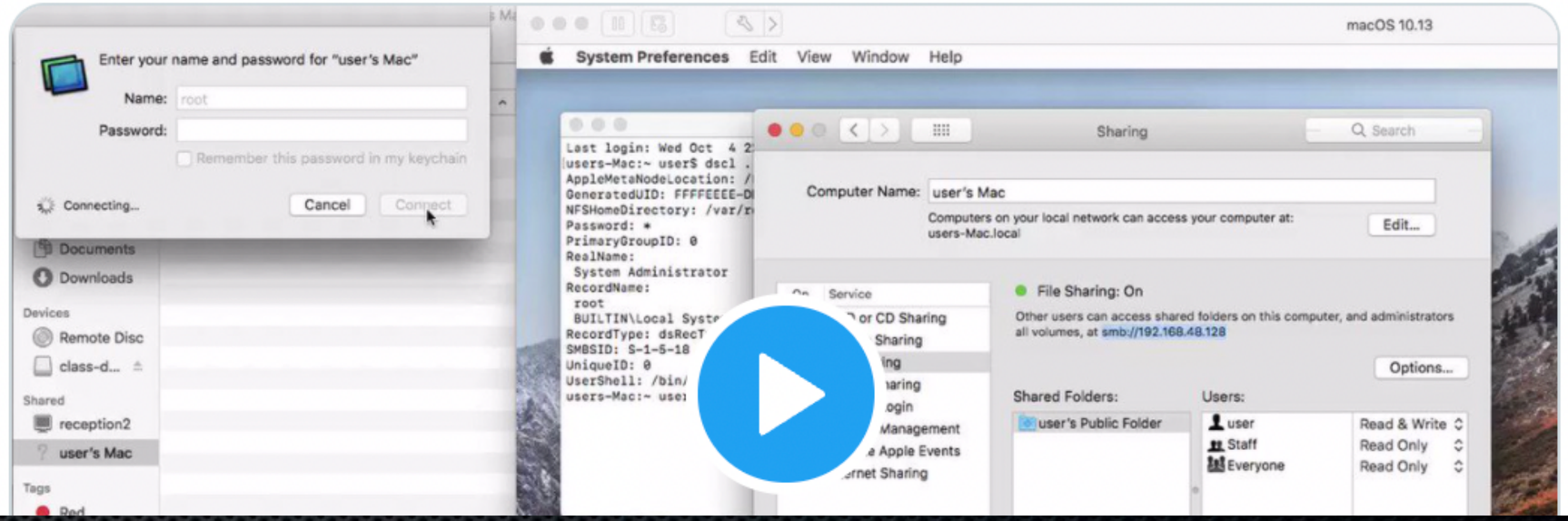
Objective by the Sea

intego

Remember this?

patrick wardle ✔
@patrickwardle

If certain sharing services enabled on target - this attack appears to work 💯 remote 🙈💀☠️ (the login attempt enables/creates the root account with blank pw) Oh Apple 🍎😷🤒🤕



macOS High Sierra

Objective by the Sea

intego

```
((err = SSLHas
 goto fail;
 goto fail;
((err = SSLHas
 goto fail;
```

...and this?

```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
                                 uint8_t *signature, UInt16 signatureLen)
{
    OSStatus        err;
    SSLBuffer       hashOut, hashCtx, clientRandom, serverRandom;
    uint8_t         hashes[SSL_SHA1_DIGEST_LEN + SSL_MD5_DIGEST_LEN];
    SSLBuffer       signedHashes;
    uint8_t         *dataToSign;
    size_t          dataToSignLen;

    ...
    if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
        goto ↓fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
        goto ↓fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto ↓fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto ↓fail;
        goto ↓fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto ↓fail;

    err = sslRawVerify(ctx,
                       ctx->peerPubKey,
                       dataToSign,              /* plaintext */
                       dataToSignLen,           /* plaintext length */
                       signature,
                       signatureLen);
    if(err) {
        sslErrorLog("SSLDecodeSignedServerKeyExchange: sslRawVerify "
                    "returned %d\n", (int)err);
        goto ↓fail;
    }
```

OS X Mavericks

Objective by the Sea

intego

Myth #2: All macOS security updates are created equal.

Uhh... No.

Objective by the Sea

intego

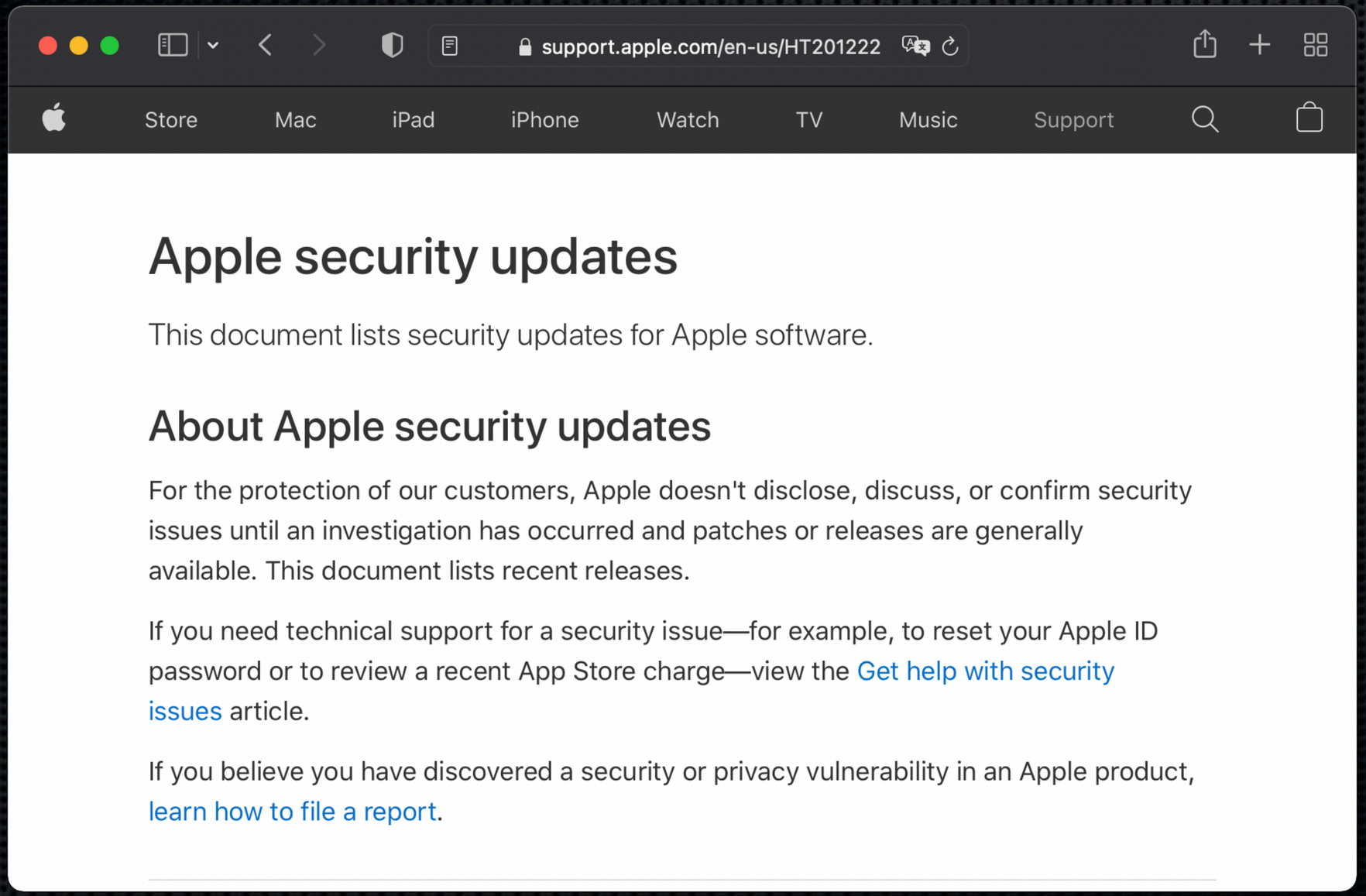
The Challenges

When Apple doesn't patch something for one or more OS…

- …is it because that vulnerability doesn't affect that OS for some reason?
- …did Apple in reality patch it, but just forgot to document it?

So we have to ask the vulnerability reporters?

- …but some are anonymous, hard to contact, or may be unwilling to discuss



Objective by the Sea

intego

	#	Gen	11.x	10.15	10.14	CVE	Researcher	Component	ACE	RA	Pr	Term	DoS	MitM	Web	Oth	Wild	Rel	Rel2C	Rel2M	Add/Up	AdUpD8	AdUpDays
2	1	11.0.1	11.0.1	2020-001C	2020-007M	2020-27914	Yu Wang of Didi Research America	AMD	√S									11/12/20	32	32	√	12/14/20	32
3	2	11.0.1	11.0.1	2020-001C	2020-007M	2020-27915	Yu Wang of Didi Research America	AMD	√S									11/12/20	32	32	√	12/14/20	32
4	3	11.0.1	11.0.1	2020-001C	2020-007M	2020-27903	Zhipeng Huo (@R3dF09) of Tencent Security Xuanwu Lab	App Store			√							11/12/20	32	32			
5	4	11.0.1	11.0.1	2020-001C	2020-007M	2020-27910	JunDong Xie and XingWei Lin of Ant Security Light-Year Lab	Audio	√									11/12/20	32	32			
6	5	11.0.1	11.0.1	2020-001C	2020-007M	2020-27916	JunDong Xie of Ant Security Light-Year Lab	Audio	√									11/12/20	32	32			
7	6	11.0.1	11.0.1	2020-001C	2020-007M	2020-9943	JunDong Xie of Ant Group Light-Year Security Lab	Audio				√						11/12/20	32	32			
8	7	11.0.1	11.0.1	2020-001C	2020-007M	2020-9944	JunDong Xie of Ant Group Light-Year Security Lab	Audio				√						11/12/20	32	32			
9	8	11.0.1	11.0.1	2020-001C	2020-007M	2020-27906	Zuozhi Fan (@pattern_F_) of Ant Group Tianqiong Security Lab	Bluetooth		√			√					11/12/20	32	32			
10	9	11.0.1	11.0.1	2021-001C	2021-001M	2020-27945	Zhuo Liang of Qihoo 360 Vulcan Team	CFNetwork Cache	√									11/12/20	81	81	√	3/16/21	124
11	10	11.0.1	11.0.1	2020-001C	2020-007M	2020-27908	JunDong Xie and Xingwei Lin of Ant Security Light-Year Lab	CoreAudio	√									11/12/20	32	32	√	12/14/20	32
12	11	11.0.1	11.0.1			2020-27909	Anonymous working with Trend Micro Zero Day Initiative, JunDong Xie and Xingwei Lin of Ant Security Light	CoreAudio	√									11/12/20	∞	∞	√	12/14/20	32
13	12	11.0.1	11.0.1	2020-001C	2020-007M	2020-9960	JunDong Xie and Xingwei Lin of Ant Security Light-Year Lab	CoreAudio	√									11/12/20	32	32	√	12/14/20	32
14	13	11.0.1	11.0.1	2020-001C	2020-007M	2020-10017	Francis working with Trend Micro Zero Day Initiative, JunDong Xie of Ant Security Light-Year Lab	CoreAudio	√									11/12/20	32	32			
15	14	11.0.1	11.0.1		2020-004M	2020-9949	Proteas	CoreCapture	√K									11/12/20	∞	*			
16	15	11.0.1	11.0.1	10.15.6		2020-9883	an anonymous researcher, Mickey Jin of Trend Micro	CoreGraphics	√									11/12/20	*	∞			
17	16	11.0.1	11.0.1			2020-10003	Tim Michaud (@TimGMichaud) of Leviathan	Crash Reporter			√							11/12/20	∞	∞			
18	17	11.0.1	11.0.1	2020-001C	2020-007M	2020-27922	Mickey Jin of Trend Micro	CoreText	√									11/12/20	32	32	√	12/14/20	32
19	18	11.0.1	11.0.1			2020-9999	Apple	CoreText	√									11/12/20	∞	∞	√U	12/14/20	32
20	19	11.0.1	11.0.1	2021-001C		2020-27937	Wojciech Reguła (@_r3ggi) of SecuRing	Directory Utility				√						11/12/20	81	∞	√	3/16/21	124
21	20	11.0.1	11.0.1			2020-9965	Proteas	Disk Images	√K									11/12/20	∞	∞			
22	21	11.0.1	11.0.1			2020-9966	Proteas	Disk Images	√K									11/12/20	∞	∞			
23	22	11.0.1	11.0.1			2020-27894	Manuel Trezza of Shuggr (shuggr.com)	Finder								√		11/12/20	∞	∞			
24	23	11.0.1	11.0.1	2020-001C	2020-007M	2020-9962	Yiğit Can YILMAZ (@yilmazcanyigit)	FontParser	√									11/12/20	32	32	√	12/14/20	32
25	24	11.0.1	11.0.1	2020-001C	2020-007M	2020-27952	an anonymous researcher, Mickey Jin and Junzhi Lu of Trend Micro	FontParser	√									11/12/20	32	32	√	12/14/20	32
26	25	11.0.1	11.0.1	2020-001C	2020-007M	2020-9956	Mickey Jin and Junzhi Lu of Trend Micro Mobile Security Research Team working with Trend Micro's Zero Da	FontParser	√									11/12/20	32	32	√	12/14/20	32
27	26	11.0.1	11.0.1	2020-001C	2020-007M	2020-27931	Apple	FontParser	√									11/12/20	32	32	√	12/14/20	32
28	27	11.0.1	11.0.1	10.15.7		2020-27930	Google Project Zero	FontParser	√								√	11/12/20	*	∞			
29	28	11.0.1	11.0.1			2020-27927	Xingwei Lin of Ant Security Light-Year Lab	FontParser	√									11/12/20	∞	∞			
30	29	11.0.1	11.0.1			2020-29639	Mickey Jin & Qi Sun of Trend Micro working with Trend Micro's Zero Day Initiative	FontParser				√						11/12/20	∞	∞	√	7/21/21	251
31	30	11.0.1	11.0.1	2020-001C	2020-007M	2020-10002	James Hutchins	Foundation				√						11/12/20	32	32			
32	31	11.0.1	11.0.1	2020-001C	2020-007M	2020-9978	Luyi Xing, Dongfang Zhao, and Xiaofeng Wang of Indiana University Bloomington, Yan Jia of Xidian Universi	HomeKit						√				11/12/20	32	32	√	12/14/20	32
33	32	11.0.1	11.0.1			2020-9955	Mickey Jin of Trend Micro, Xingwei Lin of Ant Security Light-Year Lab	ImageIO	√									11/12/20	∞	∞	√	12/14/20	32
34	33	11.0.1	11.0.1	2020-001C	2020-007M	2020-27924	Lei Sun	ImageIO	√									11/12/20	32	32	√	12/14/20	32
35	34	11.0.1	11.0.1	2020-001C	2020-007M	2020-27912	Xingwei Lin of Ant Security Light-Year Lab	ImageIO	√									11/12/20	32	32	√U	12/14/20	32
36	35	11.0.1	11.0.1	2020-001C	2020-007M	2020-27923	Lei Sun	ImageIO	√									11/12/20	32	32	√U	12/14/20	32
37	36	11.0.1	11.0.1			2020-9876	Mickey Jin of Trend Micro	ImageIO	√			√						11/12/20	∞	∞			
38	37	11.0.1	11.0.1	2020-001C	2020-007M	2020-10015	ABC Research s.r.o. working with Trend Micro Zero Day Initiative	Intel Graphics Driver	√K									11/12/20	32	32	√	12/14/20	32
39	38	11.0.1	11.0.1	2020-001C	2020-007M	2020-27897	Xiaolong Bai and Min (Spark) Zheng of Alibaba Inc., and Luyi Xing of Indiana University Bloomington	Intel Graphics Driver	√K									11/12/20	32	32	√	12/14/20	32
40	39	11.0.1	11.0.1	2020-001C	2020-007M	2020-27907	ABC Research s.r.o. working with Trend Micro Zero Day Initiative, Liu Long of Ant Security Light-Year Lab	Intel Graphics Driver	√K									11/12/20	32	32	√+√U	12/14/20	32
41	40	11.0.1	11.0.1	2020-001C	2020-007M	2020-27919	Hou JingYi (@hjy79425575) of Qihoo 360 CERT, Xingwei Lin of Ant Security Light-Year Lab	Image Processing	√									11/12/20	32	32	√	12/14/20	32
42	41	11.0.1	11.0.1	2020-001C	2020-007M	2020-9967	Alex Plaskett (@alexjplaskett)	Kernel		√		√						11/12/20	32	32	√	12/14/20	32
43	42	11.0.1	11.0.1	2020-001C	2020-007M	2020-9975	Tielei Wang of Pangu Lab	Kernel	√K									11/12/20	32	32	√	12/14/20	32
44	43	11.0.1	11.0.1	2020-001C	2020-007M	2020-27921	Linus Henze (pinauten.de)	Kernel	√K									11/12/20	32	32	√	12/14/20	32
45	44	11.0.1	11.0.1	2021-001C	2021-001M	2020-27904	Zuozhi Fan (@pattern_F_) of Ant Group Tianqong Security Lab	Kernel	√K									11/12/20	81	81			
46	45	11.0.1	11.0.1	10.15.6		2019-14899	William J. Tolley, Beau Kujath, and Jedidiah R. Crandall	Kernel						√				11/12/20	∞	∞			
47	46	11.0.1	11.0.1			2020-27950	Google Project Zero	Kernel				√					√	11/12/20	∞	∞			

Some rough numbers

- 468 total Big Sur-era vulnerabilities

- 217 vulns patched for all 3 (BS, C, & M)
- 154 vulns patched only in Big Sur
- 74 vulns patched only in Big Sur & Catalina

- 11 vulns patched in only Catalina & Mojave
- 7 vulns patched in only Catalina
- 2 vulns patched in only Mojave
- 3 vulns patched in only Big Sur & Mojave??

There’s one more thing…

Objective by the Sea

intego

“Apple is aware of a report that this issue may have been actively exploited.”

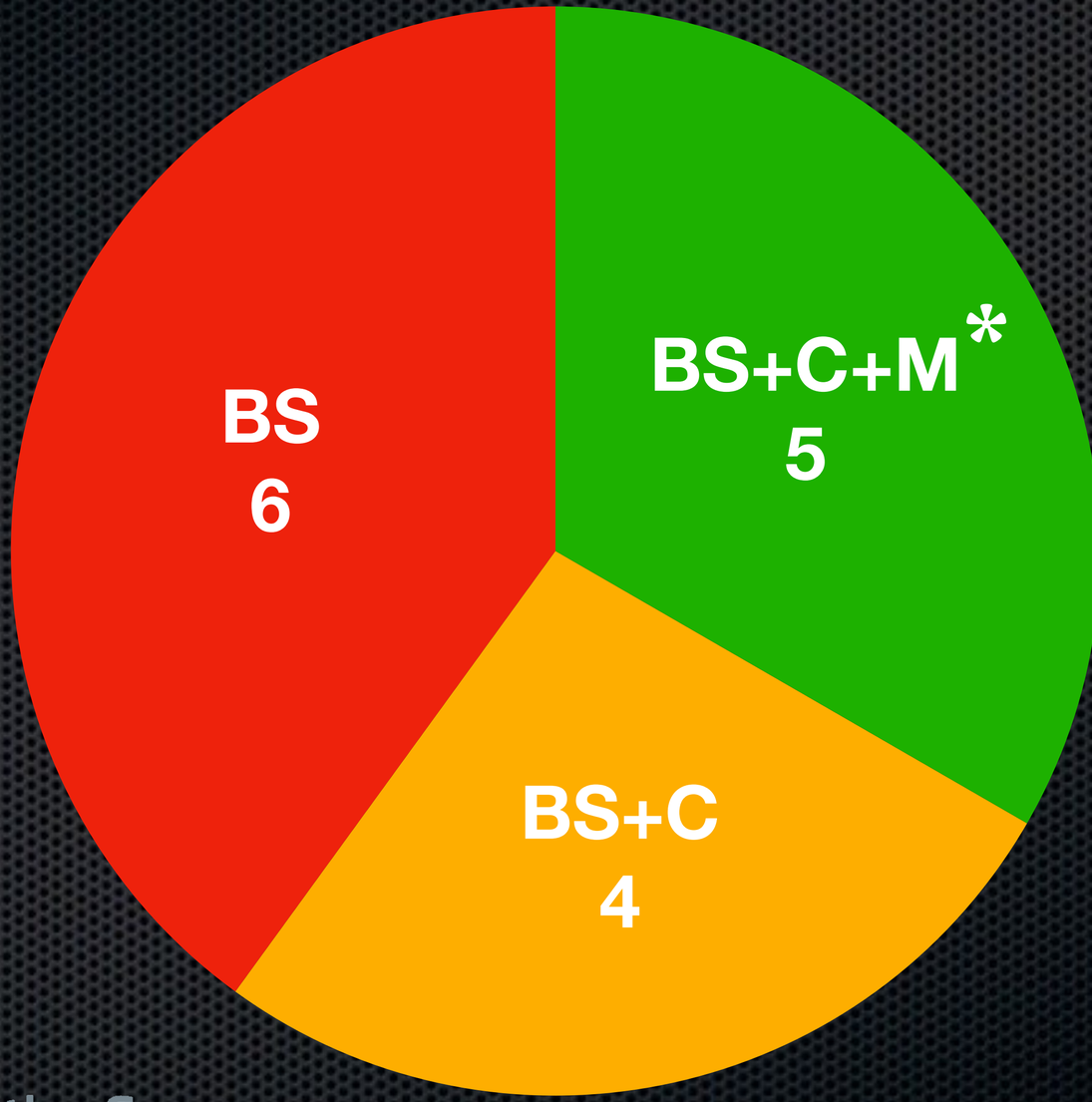
"Apple is aware of a report
that this issue may have been
actively exploited."

15 "actively exploited" vulns since Big Sur's release

Objective by the Sea

intego

15 “actively exploited” vulns since Big Sur’s release



⬅️ * Asterisk because technically one of the 5 was only patched for BS & C but didn’t apply to M, so I counted it here because every affected OS was patched

11.x	10.15	10.14	CVE	Researcher	Component
11.2	2021-001C	2021-001M	2021-1782	an anonymous researcher	Kernel
11.3.1	Safari14.1	Safari14.1	2021-30665	yangkang (@dnpushme)&zerokeeper&bia	WebKit
11.3.1	Safari14.1	Safari14.1	2021-30663	an anonymous researcher	WebKit
11.6	Safari14.1.2*	Safari14.1.2*	2021-30858	an anonymous researcher	WebKit
11.3	2021-002C	N/A	2021-30657	Cedric Owens (@cedowens)	System Preferences
11.6	2021-005C		2021-30860	The Citizen Lab	CoreGraphics
11.2	2021-006C		2021-30869	Erye Hernandez of Google Threat Analysi	XNU
11.4	2021-005C		2021-30713	an anonymous researcher	TCC
11.0.1	10.15.7		2020-27930	Google Project Zero	FontParser
11.2			2021-1871	an anonymous researcher	WebKit
11.2			2021-1870	an anonymous researcher	WebKit
11.3			2021-30661	yangkang(@dnpushme) of 360 ATA	WebKit Storage
11.0.1			2020-27950	Google Project Zero	Kernel
11.0.1			2020-27932	Google Project Zero	Kernel
11.5.1			2021-30807	an anonymous researcher	IOMobileFrameBuffer

Objective by the Sea

* Many “actively exploited” vulns were reported anonymously

intego

11.x	10.15	10.14	CVE	Researcher	Component
11.2	2021-001C	2021-001M	2021-1782	an anonymous researcher	Kernel
11.3.1	Safari14.1	Safari14.1	2021-30665	yangkang (@dnpushme)&zerokeeper&bia	WebKit
11.3.1	Safari14.1	Safari14.1	2021-30663	an anonymous researcher	WebKit
11.6	Safari14.1.2*	Safari14.1.2*	2021-30858	an anonymous researcher	WebKit
11.3	2021-002C	N/A	2021-30657	Cedric Owens (@cedowens)	System Preferences
11.6	2021-005C		2021-30860	The Citizen Lab	CoreGraphics
11.2	2021-006C		2021-30869	Erye Hernandez of Google Threat Analysi	XNU
11.4	2021-005C		2021-30713	an anonymous researcher	TCC
11.0.1	10.15.7		2020-27930	Google Project Zero	FontParser
11.2			2021-1871	an anonymous researcher	WebKit
11.2			2021-1870	an anonymous researcher	WebKit
11.3			2021-30661	yangkang(@dnpushme) of 360 ATA	WebKit Storage
11.0.1			2020-27950	Google Project Zero	Kernel
11.0.1			2020-27932	Google Project Zero	Kernel
11.5.1			2021-30807	an anonymous researcher	IOMobileFrameBuffer

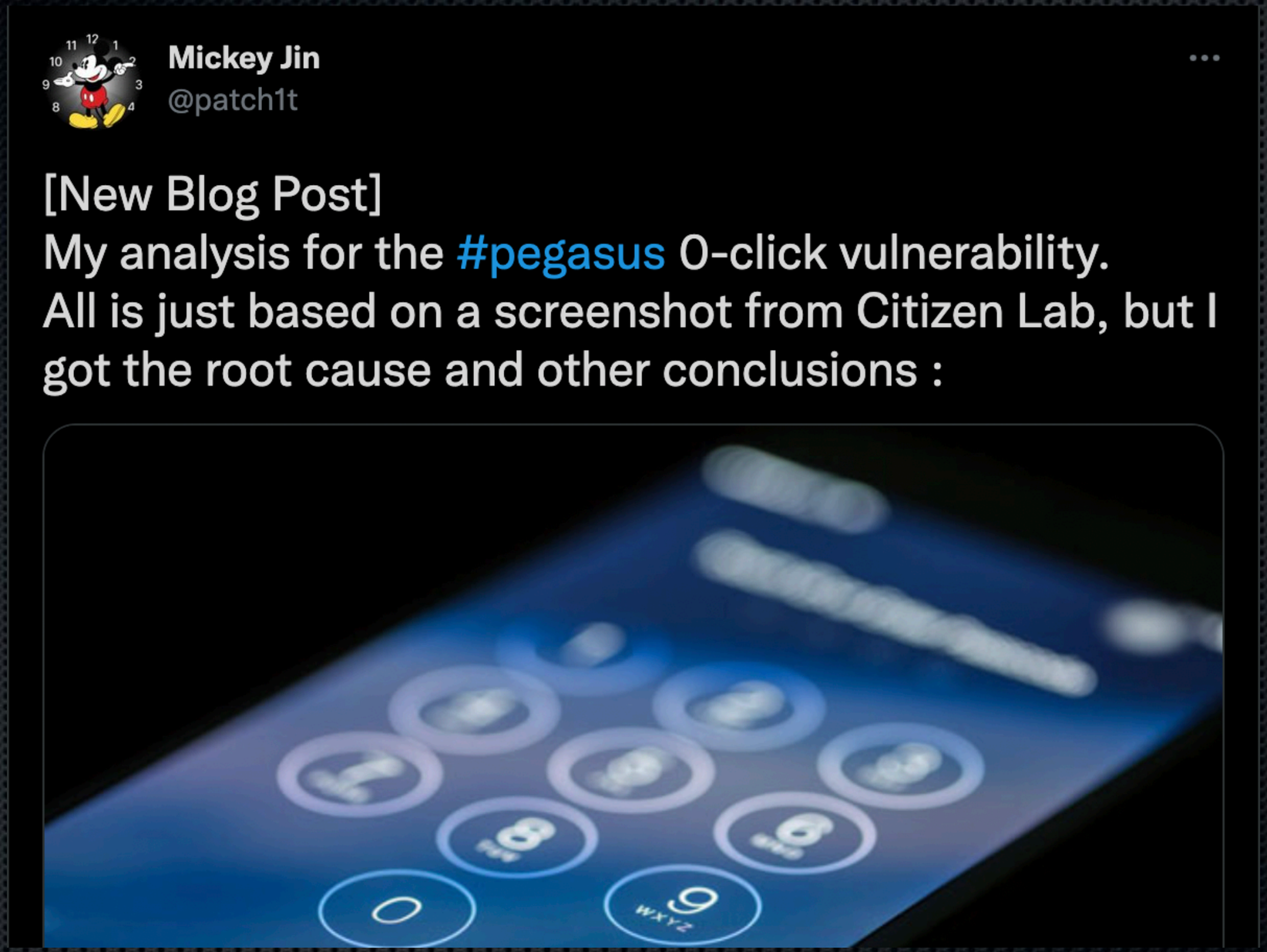
Objective by the Sea

*WebKit vulns presumably apply to all, so why weren't these actively exploited vulns patched?

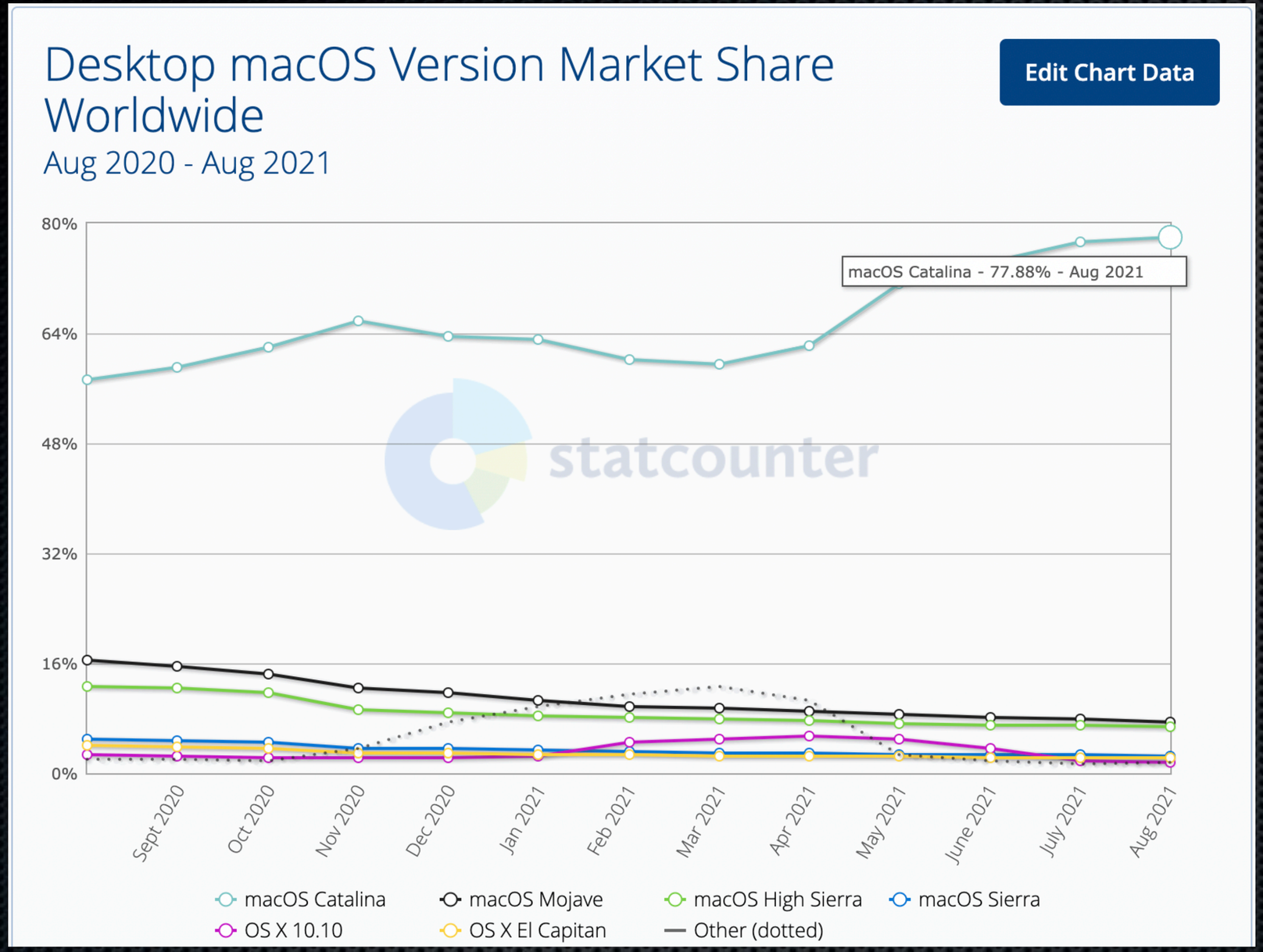
intego

11.x	10.15	10.14	CVE	Researcher	Component
11.2	2021-001C	2021-001M	2021-1782	an anonymous researcher	Kernel
11.3.1	Safari14.1	Safari14.1	2021-30665	yangkang (@dnpushme)&zerokeeper&bia	WebKit
11.3.1	Safari14.1	Safari14.1	2021-30663	an anonymous researcher	WebKit
11.6	Safari14.1.2*	Safari14.1.2*	2021-30858	an anonymous researcher	WebKit
11.3	2021-002C	N/A	2021-30657	Cedric Owens (@cedowens)	System Preferences
11.6	2021-005C		2021-30860	The Citizen Lab	CoreGraphics
11.2	2021-006C		2021-30869	Erye Hernandez of Google Threat Analysi	XNU
11.4	2021-005C		2021-30713	an anonymous researcher	TCC
11.0.1	10.15.7		2020-27930	Google Project Zero	FontParser
11.2			2021-1871	an anonymous researcher	WebKit
11.2			2021-1870	an anonymous researcher	WebKit
11.3			2021-30661	yangkang(@dnpushme) of 360 ATA	WebKit Storage
11.0.1			2020-27950	Google Project Zero	Kernel
11.0.1			2020-27932	Google Project Zero	Kernel
11.5.1			2021-30807	an anonymous researcher	IOMobileFrameBuffer

* That CVE was leveraged by Pegasus. So why wasn't it patched for Mojave? Does it not affect Mojave?



* Mickey Jin confirmed to me privately that Mojave *is* affected!



Current macOS version market share:

Big Sur & Catalina: 78%

Mojave and older: 22%

Objective by the Sea

intego

What about iOS?

- Some older iOS devices are stuck with iOS 12
- Apple is only patching “actively exploited” vulnerabilities for iOS 12
- iOS 13 isn’t getting any updates anymore
- iOS 14 is supposed to continue getting updates
- iOS 15 is the latest (but is missing two “actively exploited” iOS 14.8 patches)

* Currently, both iOS 14.8 and iOS 15 are not causing a red badge on the Settings app to prompt users to upgrade

Takeaways

- Generally speaking, the current macOS version is the safest one
  - it gets the most total patches, and the most important ones
- Avoid using *n*-1 or *n*-2 as your main macOS whenever possible

* in spite of the occasional new vulnerabilities that may be introduced, like goto fail and I Am Root

Resources

- White paper with additional details coming soon!
- The Mac Security Blog: blog.intego.com
- Follow @theJoshMeister and @IntegoSecurity

* Sign up to be notified when the white paper is available via the link at https://www.intego.com/mac-security-blog/integos-josh-long-speaking-at-obts-v4-0-mac-security-conference/ or follow @theJoshMeister and/or @IntegoSecurity & hit the bell icon to be alerted to new tweets—we'll share when the white paper is available.

Objective by the Sea

intego

Thank you!

Each of these folks provided invaluable feedback—*thanks a million!*

08Tc3wBB • Aleksandar Nikolic • an anonymous researcher • Cedric Owens • Csaba Fitzl (theevilbit) • Gabe Kirkpatrick • gorelics • Jatayu Holznagel • Lauritz Holtmann • Linus Henze • Lior Halphon • Mickey Jin (patch1t) • Mikko Kenttälä (Turmio_) • Patrick Wardle • Prakash (1lastBr3ath) • Robert • Samy Kamkar • Shivam Kamboj Dattana (Sechunt3r) • Siguza • Steffen Klee • Thijs Alkemade • Tim Michaud • Wojciech Reguła (_r3ggi) • Yiğit Can Yılmaz • YoKo Kho • Yuebin Sun • Zhipeng Huo (R3dF09) • Zuozhi Fan (pattern_F_)

Objective by the Sea

intego

@IntegoSecurity /Intego @intego_security

Questions?

Josh Long • jlong@intego.com
@theJoshMeister • theJoshMeister.com

Objective by the Sea

intego

Image credits

- Right Curly Bracket by Muneer A.Safiah CC BY 3.0
- I AM ROOT logo: Groot by Johnathon Burns; RootGate adaptation by Gaël
- I Am Root demo video loop by Patrick Wardle
- goto fail close-up from Goto Fail (Song) by James Dempsey and The Breakpoints
- goto fail larger screen shot by Synopsis
- Pegasus iPhone: iPhone by Rafael Fernandez (CC BY-SA 4.0); Pegasus by Nicolas Raymond (CC BY 2.0); composition by Joshua Long (CC BY-SA 4.0)
- Desktop macOS Desktop Version Market Share: screenshot of Statcounter site
- All other images, logos, etc. are the property of their respective owners

Objective by the Sea

intego