Heather:

Welcome to the Hurricane Labs podcast. I'm Heather, and today I have Meredith here with me to talk a little bit about Apple's latest zero day vulnerabilities. But, before we dive into them, Meredith, you wanted to talk a little bit about Apple's bug bounty program, because that has a lot to do with how people are responding to this whole situation.

Meredith:

So a few years ago, apple joined the ranks of all of the other large scale and smaller scale companies, actually that have they're known as bug bounty programs. So they've got one for, you know, your standard bones and misconfigurations as well as security bounties. And they open that up so that you didn't have to be an employee working at apple to report these things and receive a payout. Basically, you had the ability to get, I believe it was up to $1.5 million US dollar payout for a valid vulnerability. The payout was going to be staggered based on how, what severity your vulnerability was given. And a lot of people have been very unhappy with the program and the approach that apple has taken to verifying those vulnerabilities and giving credit where credit is due to the security researchers or those who have found vulnerabilities, including working with them to remediate the issue or correctly attributing who discovered the issue and why they are releasing this patch in the next either, you know, security update for Mac OS or feature update for iPad or less, whatever it may be.

Meredith:

Right. And I will say that for everybody who knows me, they know that I am the first to jump on most new apple products and see if they are worthwhile or beneficial or not. But you know, they're not a perfect company. They do far better than some other companies when it comes to this. But with how young this program is, people are quickly losing faith in their statements about Apple caring about security and privacy just based on the last year and a half or so that they've rolled this program out. And people are third parties, and now seeing their lack of transparency.

Heather:

So now what is happening with these zero days?

Meredith:

A few weeks ago, things kind of blew up in the Twitterverse because a security researcher reach out and tweeted about a blog post that found saying, "I reported four zero day vulnerabilities that should be considered critical to Apple." I think it was within the first few months of the year, the first half of the year, they reported four, three of them are still present. And apple had previously fixed one and refused to give them credit where credit was due. That person said they reached out to Apple, Apple apologized and said it was merely a processing error, and then promise listed in the security content in the next update. There've been three releases each time and they broke their promise each time.

Heather:

But what all is affected by these vulnerabilities?

Meredith:

So on your iPhone and iPad, anything that uses the game center apps installed via the app store, which is Apple's verified accredited way to install an application. It's very hard to do this otherwise without

jailbreaking your device. So it's to prevent, you know, malicious applications from passing through code checks. So this is designed to be a security feature, but one of those four zero days was that basically any app installed from the app store could potentially have access to some of the user's data, including their apple ID, email address, the full name associated. So that's personally identifiable information (PII), and then basically file system read access for that device, as well as grabbing access of the, what they call the core duet database, which is basically list of contexts from mail iMessage or texts, and like any other third party messaging apps you may have installed on there.

Meredith:

So, you know, that would be Facebook messenger, WhatsApp, applications like those, and then evidently metadata about the user's interactions with those contacts, including like times that you've sent messages, statistics of how often you're reaching out to them. And then, additionally, like any like images or URLs that would go along with those messages. And then additionally, full re-access to like the contact book and like favorites like database or the speed dial database is what they call it. And that's got, you know, your contact photos. And then other information like the created and edited dates, the author of this vulnerability did say that they recently checked with iOS 15 and that one must've been quietly patched. And that is one of the ones that wasn't correctly attributed to them,

Heather:

That sort of attribution. Why is that important when it comes to third party vulnerability disclosures?

Meredith:

So there are some security research companies out there that their entire job, or they have people whose entire day to day is looking at various companies softwares who have bug bounties and their company is essentially a group of people who work on these bug bounties insecurity bounties. And a lot of them basically work on commission from the verification of these. So if this isn't attributed to them or Apple isn't willing to provide the payout, they don't get paid, they don't get recognized for their work. And, you know, the month they've spent dipping into this is basically down the drain from their end. They've done the job that somebody at Apple should have done, and then didn't get the payout that they should have received.

Heather:

You know, these programs, I mean, they're designed right to benefit the company to end this, you know, by extension their customers, their clientele. So it's, I guess it's, you know, it's important that they're, you know, they're making it worth people's while, you know, it's time-consuming and I feel like the companies should be, you know, have at least a little bit of grace and gratitude that someone is like, "Hey, before, you know, shit really hits the fan. Maybe you should be aware that ABC is available."

Meredith:

Yeah, like that is the ultimate ideal that for some reason it never gets upheld.

Heather:

So like back onto the zero days, there was not an update except for the one that might've been patched. You said.

Meredith:

Yeah, it looks like that one was very recently silently patched looking at the Apple security update, it looks like the, yeah, the games center zero day is patch, but it doesn't appear to be, doesn't appear to have been attributed or documented. That being said, I don't feel comfortable with the fact that I can't find it on the documentation page. The security researcher has verified that they can no longer reproduce the issue, but the lack of transparency from Apple does not give me much trust in the matter.

Heather:

Well, I mean, what are the big things that they could do to win back that respect–that faith?

Meredith:

The first thing I think would be to back credit, like the proper attribution to vulnerabilities. They've got a very good, you know, Apple Security Updates page, you know, it's constantly kept up to date and they list out the security updatem, what the effective product is, whether that's hardware or software, the version number of the software that contains the correct patch and the release date. When you click into them, some do have proper attributions, some do not. So adding that in there and reaching out to these researchers and for those who didn't receive their, you know, compensation, whether it be just monetary, some have said, I don't want money, I'd just like this to be attributed to my name. So fulfilling those requests, I think would be a very good step. And then being far more transparent. I would prefer to not see apple go the route where things get so big and so bad that every other day they're coming up with a new zero day that is critical, that needs a patch. And we'll see things, you know, as a zero day for months on end or weeks on end, without much communication from the company.

Heather:

What does it mean for general users for as like, what they have to do to protect themselves, is that lead line box time for their devices.

Meredith:

Okay. So this is like my own little Meredith soap box here, but I know that, you know, people are very attached to the operating system of their phones or their computers or what they primarily primarily run. You know, are you Windows? Are you Linux? Are you Mac OS? But one of the most important things to do is to look at the patch notes for something. And if it doesn't appear to impact anything that you need to do, patch early and patch often, so that when a vulnerability is discovered in something that's two or three versions old, you're not sitting out there vulnerable to that and spending hours and hours of downtime, whether it's on your work or personal device, when you could have just done them, spaced out, the way that they had attended. That being said, you know, it's not perfect. Sometimes we'll push out a patch that isn't perfectly stable, but sometimes sacrificing functionality for security is going to have to have, is going to have to be done.

Heather:

So hitting the, not today, maybe shouldn't be happening?

Meredith:

Correct. Apple does a good job at, you know, older operating systems keeping their older operating systems up to date, and they'll push out the same security patches across multiple versions of, you

know, Big Sur, Catalina, whatever it may be. So that each major version is patched. But when it comes down to, you know, just you're on something so old, and you know, I'm going to date myself here and go all the way back to Snow Leopard, no snow leopard doesn't have security patches anymore. You need to, well, actually at that point, you may just want to buy a new device, but

Heather:

Alright, well, that's all we have for today. Thanks for joining us. Next time, Meredith will be rejoining us with Tom, and we're going to be talking a little bit about physical security. So stay tuned, until next time, stay safe.