Apple takes flak for disputing iOS security bombshell dropped by Google

reader comments

178 with 110 posters participating

Share this story

Apple is taking flak for disputing some minor details of last week's bombshell report that, for at least two years, customers' iOS devices were vulnerable to a string of zeroday exploits, at least some of which were actively exploited to install malware that stole location data, passwords, encryption keys, and a wealth of other highly sensitive data.

Google's Project Zero said the attacks were waged indiscriminately from a small collection of websites that "received thousands of visitors per week." One of the five exploit chains Project Zero researchers analyzed showed they "were likely written contemporaneously with their supported iOS versions." The researcher's conclusion: "This group had a capability against a fully patched iPhone for at least two years."

Earlier this week, researchers at security firm Volexity reported finding 11 websites serving the interests of Uyghur Muslims that the researchers believed were tied to the attacks Project Zero identified. Volexity's post was based in part on a report by TechCrunch citing unnamed people familiar with the attacks who said they were the work of nation—likely

China—designed to target the Uyghur community in the country's Xinjiang state.

Breaking the silence

For a week, Apple said nothing about any of the reports. Then on Friday, it issued a statement that critics are characterizing as tone-deaf for its lack of sensitivity to human rights and an overfocus on minor points. Apple officials wrote:

> *Last week, Google published a blog about vulnerabilities that Apple fixed for iOS users in February. We've heard from customers who were concerned by some of the claims, and we want to make sure all of our customers have the facts.*
>
> *First, the sophisticated attack was narrowly focused, not a broad-based exploit of iPhones "en masse" as described. The attack affected fewer than a dozen websites that focus on content related to the Uighur community. Regardless of the scale of the attack, we take the safety and security of all users extremely seriously.*
>
> *Google's post, issued six months after iOS patches were released, creates the false impression of "mass exploitation" to "monitor the private activities of entire populations in real time," stoking fear among all iPhone users that their devices had been compromised. This was never the case.*
>
> *Second, all evidence indicates that these website attacks were only operational for a brief period, roughly two months, not "two years" as Google implies. We fixed the vulnerabilities in question in February – working extremely quickly to resolve the issue just 10 days after we learned about it. When Google approached us, we were already in the process of fixing the exploited bugs.*
>
> *Security is a never-ending journey and our customers can be*

> *confident we are working for them. iOS security is unmatched because we take end-to-end responsibility for the security of our hardware and software. Our product security teams around the world are constantly iterating to introduce new protections and patch vulnerabilities as soon as they're found. We will never stop our tireless work to keep our users safe.*

One of the things most deserving of criticism was the lack of sensitivity the statement showed for the Uyghur population, which over the past decade or longer has faced hacking campaigns, internment camps, and other forms of persecution at the hands of the Chinese government. Rather than condemning an egregious campaign perpetrated on a vulnerable population of iOS users, Apple seemed to be using the hacking spree to assure mainstream users that they weren't targeted. Conspicuously missing from the statement was any mention of China.

Nicholas Weaver, a researcher at UC Berkeley's International Computer Science Institute, summed up much of this criticism by tweeting: "The thing that bugs me most about Apple these days is that they are all-in on the Chinese market and, as such, refuse to say something like 'A government intent on ethnic cleansing of a minority population conducted a mass hacking attack on our users.'"

> *The thing that bugs me most about Apple these days is that they are all-in on the Chinese market and, as such, refuse to say something like "A government intent on ethnic cleansing of a minority population conducted a mass hacking attack on our users." https://t.co/ACMhtpN53H*
>
> *— Nicholas Weaver (@ncweaver) September 6, 2019*

The statement also seemed to use the fact that "fewer than a dozen" sites were involved in the campaign as another

mitigating factor. Project Zero was clear all along that the number of sites was “small” and they had only a few thousand of visitors each month. More importantly, the size of the campaign had everything to do with decisions made by the attackers and little or nothing to do with the security of iPhones.

Two months or two years?

One of the few factual assertions Apple provided in the statement is that the websites were probably operational for only about two months. A careful parsing of the Project Zero report shows researchers never stated how long the sites were actively and indiscriminately exploiting iPhone users. Rather, the report said, an examination of the five attack chains made up of 14 separate exploits suggested that they gave the hackers the ability to infect fully up-to-date iPhones for at least two years.

These points prompted satiric tweets similar to this one from Juan Andrés Guerrero-Saade, a researcher at Alphabet-owned security firm Chronicle: “‘It didn’t happen the way they said it happened, but it happened, but it wasn’t that bad, and it’s just Uyghurs so you shouldn’t care anyways. No advice to give here. Just move along.’”

> *Wow @apple…*
>
> *‘It didn’t happen the way they said it happened, but it happened, but it wasn’t that bad, and it’s just Uyghurs so you shouldn’t care anyways. No advice to give here. Just move along.’*
>
> *— J. A. Guerrero-Saade (@juanandres_gs) September 6, 2019*

Satire aside, Apple seems to be saying that evidence suggests that the sites that Google found indiscriminately exploiting the iOS vulnerabilities were operational for only two months.

Additionally, as reported by ZDNet, a researcher from security firm RiskIQ claims to have uncovered evidence that the websites didn't attack iOS users indiscriminately, but rather only visitors from certain countries and communities.

If either of those points are true then it's worth taking note, since virtually all media reports (including the one from Ars) have said sites indiscriminately did so for at least two years. Apple had an opportunity to clarify this point and say precisely what it knows about active use of the five iPhone exploit chains Project Zero found. But Friday's statement said nothing about any of this, and Apple representatives didn't respond to a request to comment for this post. A Google spokesman said he didn't know precisely how long the small collection of websites identified in the report were operational. He said he'd try to find out, but didn't respond further.

In a statement, Google officials wrote: "Project Zero posts technical research that is designed to advance the understanding of security vulnerabilities, which leads to better defensive strategies. We stand by our in-depth research which was written to focus on the technical aspects of these vulnerabilities. We will continue to work with Apple and other leading companies to help keep people safe online."

A missed opportunity

Former NSA hacker and founder of the firm Rendition Infosec Jake Williams told Ars that ultimately, the time the exploit sites were active is immaterial. "I don't know that these other 22 months matter," he explained. "It feels like their statement is more of a straw man to deflect away from the human rights abuses."

Also missing from Apple's statement is any response to the blistering criticism the Project Zero report made of Apple's development process, which the report alleges missed

vulnerabilities that in many cases should have been easy to catch with standard quality-assurance processes.

“I’ll investigate what I assess to be the root causes of the vulnerabilities and discuss some insights we can gain into Apple’s software development lifecycle,” Project Zero researcher Ian Beer wrote in an overview of last week’s report. “The root causes I highlight here are not novel and are often overlooked: we’ll see cases of code which seems to have never worked, code that likely skipped QA or likely had little testing or review before being shipped to users.”

Another key criticism is that Apple’s statement has the potential to alienate Project Zero, which according to a Google spokesman has to date privately reported more than 200 vulnerabilities to Apple. It’s easy to imagine that it wasn’t easy for Apple to read last week’s deep-dive report publicly documenting what is easily the worst iOS security event in its 12-year history. But publicly challenging a key ally on such minor details with no new evidence does not create the best optics for Apple.

Apple had an opportunity to apologize to those who were hurt, thank the researchers who uncovered systemic flaws that caused the failure, and explain how it planned to do better in the future. It didn’t do any of those things. Now, the company has distanced itself from the security community when it needs it most.

https://arstechnica.com/?p=1563931