Zero-day in Sign in with Apple

May 30, 2020

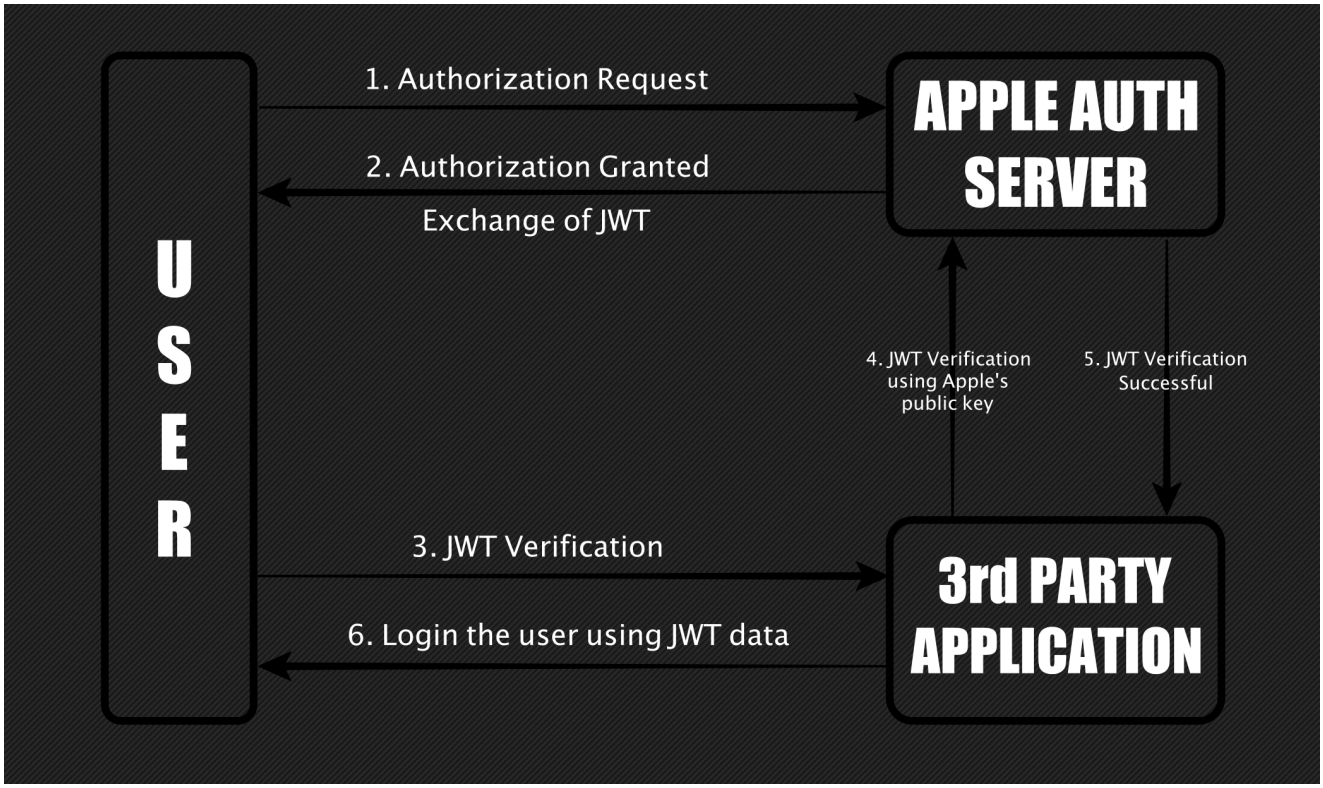
What if I say, your Email ID is all I need to takeover your account on your favorite website or an app. Sounds scary, right? This is what a bug in `Sign in with Apple` allowed me to do.

In the month of April, I found a zero-day in `Sign in with Apple` that affected third-party applications which were using it and didn't implement their own additional security measures. This bug could have resulted in a **full account takeover of user accounts** on that third party application irrespective of a victim having a valid Apple ID or not.

> For this vulnerability, I was paid $100,000 by Apple under their Apple Security Bounty program.

Technical Details

The `Sign in with Apple` works similarly to OAuth 2.0. There are two possible ways to authenticate a user by either using a `JWT (JSON Web Token)` or a `code` generated by the Apple server. The code is then used to generate a JWT. The below diagram represents how the JWT creation and validation works.



In the 2nd step, while authorizing, Apple gives an option to a user to either share the Apple Email ID with the 3rd party app or not. If the user decides to hide the Email ID, Apple generates its own user-specific Apple relay Email ID. Depending upon the user selection, after successful authorization, Apple creates a JWT which contains this Email ID which is then used by the 3rd party app to login a user.

A decoded JWT's payload looks like this:

```
{
  "iss": "https://appleid.apple.com",
  "aud": "com.XXXX.weblogin",
  "exp": 158XXXXXXX,
  "iat": 158XXXXXXX,
  "sub": "XXXX.XXXXX.XXXX",
  "c_hash": "FJXwx9EHQqXXXXXXXX",
  "email": "contact@bhavukjain.com", // or "XXXXX@privaterelay.appleid.com"
  "email_verified": "true",
  "auth_time": 158XXXXXXX,
  "nonce_supported": true
}
```

****BUG****

I found I could request JWTs for any Email ID from Apple and when the signature of these tokens was verified using Apple's public key, they showed as valid. This means an attacker could forge a JWT by linking any Email ID to it and gaining access to the victim's account.

Sample Request (2nd step)

```
POST /XXXX/XXXX HTTP/1.1
Host: appleid.apple.com

{"email":"contact@bhavukjain.com"}
```

Here on passing any `email`, Apple generated a valid JWT (id_token) for that particular Email ID.

Sample Response

```
{
  "authorization" : {
    "id_token" : "eyJraWQiOiJlWGF1bm1MIiwiYWxnIjoiUlMyNTYifQ.XXXXX.XXXXX",
    "grant_code" : "XXX.0.nzr.XXXX",
    "scope" : [ "name", "email" ]
  },
  "authorizedData" : {
    "userId" : "XXX.XXXXX.XXXX"
  },
  "consentRequired" : false
}
```

The impact of this vulnerability was quite critical as it could have allowed full account takeover. A lot of developers have integrated `Sign in with Apple` since it is mandatory for applications that support other social logins. To name a few that use `Sign in with Apple` - Dropbox, Spotify, Airbnb, Giphy (Now acquired by Facebook). These applications were not tested but could have been vulnerable to a full account takeover if there weren't any other security measures in place while verifying a user.

Apple also did an investigation of their logs and determined there was no misuse or account compromise due to this vulnerability.

A huge thanks to the Apple Security Team.

Thanks for the read, see you in next article :)

ALSO ON **BHAVUKJAIN.COM**

Zomato Account Takeover using …

5 years ago · 1 comment

This was an issue, I reported to Zomato a few months back where an …

Extracting Sensitive PII From a Tracking …

5 years ago · 3 comments

While checking out Grab Parcel website, I found a link that looked a bit …

Account Takeover Due to Misconfigured …

5 years ago · 4 comments

The mobile applications that uses Login with Facebook or Login with Google, I've …

Z A

3

W a a

What do you think?

2918 Responses

51 Comments

Login

G

Join the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS

Name

28 Share

Best Newest Oldest

TikkyMikk

2 months ago edited

She's not different than her trashy brother

yD.2632N.US\iG9105dM

54 0 • Reply • Share ›

BG

Bhaskar g

3 years ago

Please add the dates when you reported and also patched date..... thanks!

35 2 • Reply • Share ›

M

MOMO

3 years ago

Did apple hired an intern to develop this feature?

10 0 • Reply • Share ›

W

Well...

3 years ago edited

~~They were kind of warned by the OpenID Foundation almost one year ago... but yeah... this is Apple we are talking about...~~

~~https://openid.net/2019/06/...~~

Nvmind, they actually did act upon it:
https://openid.net/2019/09/...
My bad

Great Job! 👍

Sponsored 4 0 • Reply • Share ›

Lubang terdalam di bumi telah terbuka setelah peneliti menemukan fossil misterius

Story To Hear

Wanita ini dipaksa keluar dari restoran, karena mereka tidak mengetahui siapa sebenarnya wanita ini

Kingdom Of Men 2 1 • Reply • Share ›

Seorang istri menangkap benda aneh dari ari, ketika suaminya melihat benda tersebut ia berteriak

Women's Method

16 foto hasil belanja online yang akan membuat anda tertawa

The Family Breeze 0 1 • Reply • Share ›

30 dari Wanita Tercantik Di Dunia Sepanjang Sejarah

Womentales.com

14 10 • Reply • Share ›

Kekayaan bersih J.K. Rowling membuat keluarganya tercengang

The Travel Breeze

5 3 • Reply • Share ›

Onne van Dijk → Well...

3 years ago

Come on, at least also post the follow up from three months later, they worked together for the final release.
https://openid.net/2019/09/...

Well → Onne van Dijk

3 years ago

Thanks for bringing it up and correcting my post, knowing the company, I wouldn't expect Apple to fix or act upon these things. But glad they did.

Roboman

3 years ago

I like dark themes but your diagram is simply unreadable.

14 10 • Reply • Share ›

Jolly Roger → Roboman

3 years ago

Nah. Looks fine here.

5 3 • Reply • Share ›

Jayden Pearse → Jolly Roger

3 years ago

It only looks good for certain displays and is completely illegible on others.

0 0 • Reply • Share ›

Pierre-Yves Lebrun

3 years ago edited

Congrats, I'd have two questions:

- how a company like Apple could make such a basic mistake?
- seriously, $100,000 just for this?!

3 2 • Reply • Share ›

Dat Boi → Pierre-Yves Lebrun

3 years ago edited

Hindsight is 2020, you call it basic after reading this article but you probably wouldn't spot it while developing before this article.

12 2 • Reply • Share ›

PL

Pierre-Yves Lebrun → Dat Boi

3 years ago

Well it could be I missing something but to me it sounds like Apple literally had an endpoint generating JWTs for any account without any other check than the original authorization step

6 0 • Reply • Share ›

Carlos Ortigoza Dempster →

Pierre-Yves Lebrun 3 years ago

That's why Apple paid 100k "just for this" :)

8 0 • Reply • Share ›

DB

Dat Boi → Pierre-Yves Lebrun

3 years ago

Yes, there's also thousands of "basic" things that could go wrong in terms of security, miss one of them and you could compromise the whole system, and people will wonder how you missed something so "basic".

1 2 • Reply • Share ›

N

Nate → Dat Boi

3 years ago

The distinction you're missing is that out of these *thousands* of basic things, some of them have, or should have, extreme priority over others. It's fair to say Apple isn't exactly innovative when it comes to web based development, but this is actually a bit stunning. They definitely ripped dude off too. Not just accounting for the liable damages recovered, OP did the work of multiple teams inside Apple and couldn't get an intern's salary.

2 1 • Reply • Share ›

Jonas N → Pierre-Yves Lebrun

3 years ago

I think the bounty is set by how easy it is to exploit and this bug looks particularly basic in that regard.

2 0 • Reply • Share ›

A

Anime-kun → Pierre-Yves Lebrun

a year ago

"seriously, $100,000 just for this?!"
bounty is determined by various factors, for example:
- how easy is it to exploits.
- the damage that can occur by exploiting this vul (imagine automating a list

of emails and taking the associated account using this method).

in real life we value things buy quality not by how hard or how long it takes to obtain, nobody cares if you worked in a vul for years and how advanced it's if the effect is almost neglectable, same goes in every field.

0 0 • Reply • Share ›

Richard Liu

3 years ago edited

Not coding for Sign-In-with-Apple and from your description I can't understand how the bug works. How can you get the JWT using forged email, if it needs authorization when you send the request ?

1. Apple didn't request for authorization at all and let you request for a signed JWT using any email address.

2. You authorize with your own Apple ID first, then change the email address in granted JWT.

If you meant the later, then this bug is in step 4, that Apple server didn't verify the email address with the previous request. In that case I'd say the easiest way to patch this bug is just padding the email address string after the authentication body when generating hash, so that hash code will be invalid if you change the email string.

However, this attack is all about getting a forged JWT to be verified at step 5 and the server logs you in at step 6. And it means that the 3rd party app server did not know the whole process before it receives forged JWT in step 4. So the app server just assumes that who sent this is trusted, and skips all transactions to check basic identity of the client, like the API version, before the whole process begins.

I must say it's not a good practice for the 3rd party app server either.

2 1 • Reply • Share ›

Jonas N

3 years ago

Wow, I can imagine that bounty because even I understand the bug and the implications from this short blog post. That is incredible. Congratulations!

1 0 • Reply • Share ›

Pradeep Chauhan

3 years ago

very lucky

1 0 • Reply • Share ›

Peter Marreck

3 years ago

so how exactly did Apple mitigate this in the interim?

1 0 • Reply • Share ›

wulymammoth → Peter Marreck
3 years ago

They don't mitigate. They fix it. When you report a zero day to any bounty, you agree not to release the vulnerability or write about it until it is patched/fixed. Such is the case here

4 0 • Reply • Share ›

M

Matte'
3 years ago

Just wow

1 0 • Reply • Share ›

David Waite
3 years ago

Are you using a different definition of "Zero Day" than I am familiar with? There is no evidence that this was exploited.

4 7 • Reply • Share ›

SN

Steven Noyes → David Waite
3 years ago

I may be wrong but...

My understanding is a zero-day is a flaw the vendor is aware of but there is no patch in place. The flaw does not have to be in the wild or being exploited. So once Apple is notified of the flaw, it is a zero-day until such a point the flaw is patched.

5 0 • Reply • Share ›

BG

Brandon Guerrero → Steven Noyes
3 years ago edited

"I may be wrong but..." yes Steven you are wrong. A Zero Day means it is in the wild and previously undiscovered. Zero Days are exploited. Check exploit-db.com for real ones and https://en.wikipedia.org/wi... for a decent description of what a Zero Day is. I agree with David

0 5 • Reply • Share ›

AD

Alex Datsko → Brandon Guerrero
3 years ago

No, you are wrong by assuming a 0day vulnerability has to be exploited in the wild to be considered 0day. A zero-day vulnerability just means a bug has been found that can be confirmed exploitable by a researcher/hacker, but info has not been released to the public yet, and the vendor has not had time to patch it yet (usually they have not even been informed of it

it yet (usually they have not even been informed of it yet). It generally is referred to as a 0day exploit, which means someone has written a working proof of concept exploit, but has not submitted it publicly. It has meant the same thing for 25+ years...

Even on the wikipedia page you linked, it mentions:

A zero-day (also known as 0-day) vulnerability is a computer-software vulnerability that is unknown to, or unaddressed by, those who should be interested in mitigating the vulnerability (including the vendor of the target software). Until the vulnerability is mitigated, hackers can exploit it to adversely affect computer programs, data, additional computers or a network.[1] An exploit directed at a zero-day is called a zero-day exploit, or zero-day attack.

A 0day is no longer 0day once it has been disclosed to the developer and assumedly they have patched or disabled it (or are working on a patch). Before that, it is still 0day because the vulnerability is unknown of, or at least it is not known to have been exploited in the wild (it may or may not have been, in actuality, the only thing that it declares is that the vulnerability is unknown to the public).

5 0 • Reply • Share ›

P

Pmarsh111 → Brandon Guerrero

3 years ago

Re-read the Wikipedia definition. There's no mention of the vulnerability needing to be exploited to call it zero day.

3 0 • Reply • Share ›

Pure → David Waite

3 years ago

David, you have no clue what you are talking about

4 1 • Reply • Share ›

A

Anime-kun → Pure

a year ago

I lost brain celling reading this thread.

0 0 • Reply • Share ›

RK

Rajesh Kumawat

3 years ago

One of the Best article to come across in 2020

1 2 • Reply • Share ›

BB

Basant Bhandari

4 months ago

<h1>hacked</h1>

0 0 • Reply • Share ›

NB

Nizamuddin Badhara

2 years ago

How you found endpoint api for apple jwt token generate by passing email id

,

Please help us

0 0 • Reply • Share ›

тролльсостажем

3 years ago

Forged token will never have a proper `aud` and I do not think ANY app was actually in danger

0 0 • Reply • Share ›

Vishal Surelia

3 years ago

Nice finding 👍

0 0 • Reply • Share ›

Charles Beyer

3 years ago

Of course they found no evidence of this hack being used ..... :(:)

0 0 • Reply • Share ›

Ujjwal Basnyat

3 years ago

month ago, I was trying to find kinda similar bug leads to full account takeover of user accounts on Login with Facebook but unfortunately I got nothing or maybe I choose wrong platform. POOR ME :(

0 0 • Reply • Share ›

BI

Baakñ. Igná

3 years ago

Quando eu crescer quero ser igual a você

0 0 • Reply • Share ›

HUNTER

3 years ago

Welldone Buddy Just Share Video POC!

0 0 • Reply • Share ›

Michel Rondberg

3 years ago

I'm using this type of login, so a big thank you for spotting this!

0 0 • Reply • Share ›

dasiths

3 years ago

Just to be clear this only affects the id_token and not the access_token? Does apple return both if requested (either via implicit or auth code flow)?

0 0 • Reply • Share ›

This comment was deleted.

Paul Brittain Guest

3 years ago

That's not how OAuth works

0 0 • Reply • Share ›

Male Sensitivity

3 years ago

Thanks for sharing this! I'm trying to learn this stuff for the first time and I feel like I'm twenty years behind :)

0 0 • Reply • Share ›

Bhavuk Jain

contact@bhavukjain.com Full stack developer interested in Web and Mobile Security.

Andrey Upadyshev

3 years ago

Thank you for great article and for the finding!
Do I understand correctly that Apple JWT is not a standard JWS (signed) nor JWE (encrypted) and thAt they have inplemented their own signing scheme on top of plain JWT? Also do they have a header part of JWT or it's payload only? If you have, could you please post an example of the whole Apple JWT on the wire?
Thank you!

0 0 • Reply • Share ›

stevefan1999

3 years ago

Apple: I became the villain I swore to destroy

0 0 • Reply • Share ›

Alexander Asis Brown

3 years ago

Not all heroes fight the coronavirus.

0 0 • Reply • Share ›

Matt

3 years ago

Any relation to the skypetoken_asm issue that MSFT patched?
CloudFlare is also relying on JWT, any risk there?