#10284 2-Factor-Authentication Bypass via Voicemail Exploit

zero reported a bug to Yahoo!. show raw · 18 days ago

Assumptions/Pre-requisites for the attack to take place:

- The attacker has the victims mobile number (attached to Yahoo Mail)
- The attacker has the victims Yahoo email and password
- The attacker must have a spoofcard / Caller ID spoofer (e.g. Spoofcard.com works for this)

1. Attacker logs into the Yahooaccount of the victim via any of Yahoo's authentication flows. E.g. https://mail.yahoo.com.
2. The attacker must quickly initiate a call with the victim, to their phone number and potentially keep them on for the next 1-3 minutes.
3. When the attacker logs in, the attacker must quickly check the option to send a call instead of a text to the victims phone. After checking this, the attacker can then issue the 2FA token via Phone whilst still on the phone with the victim.
4. Since the attacker is on the phone with the victim, the Yahoo 2FA code will be sent to the victims voicemail (which is the flaw which needs to be mitigated). The attacker can then end the call with the victim and finally continue with their 2FA bypass.
5. In Australia, service providers (such as Optus) have a specified voicemail number, as do many other providers. In this case, a quick google search brings us the voicemail mobile number to call for all Optus phones: +61411000321
6. In the Spoofcard panel, I would merely spoof my victims mobile number, and call Optus's voicemail number (+61411000321)
7. Due to the spoof, the provider will let me into the voicemail immediately and I would be able to obtain the pin and then login, essentially bypassing the presence of two-factor authentication.

I understand that what I have described above has a few pre-requisites, the major ones being the dependence of getting access to ones voicemail. I conducted tests on the top 3 telco's in Australia (as they were the only ones I had in reach) and 2/3 were vulnerable to this sort of spoofing attack. (Gaining access to voicemail without a pin)

Even though these telco's are also at fault in this exploit, it is unknown how long they may take to fix this issue, and hence it can be Yahoo's responsibility as they have the ability to prevent 2FA codes going to voicemail in their 2FA flow.

The only way I see this vulnerability/exploit being mitigated is by configuring the Yahoo caller which sends the 2FA pin to **not** leave a voicemail under any circumstances. There is no need for the tokens to go to voicemail, in my opinion.

Thanks,
I think this is urgent, please reply shortly

zero posted a comment. 17 days ago

I have confirmed the above exploit works on the following Australian networks:

Optus, Optus Business, Virgin Mobile, Amaysim, Vodafone, TPG, Vaya, LiveConnected, Crazy Johns Mobile, Dodo and basically any other network using Optus's reseller service.

Due to such a wide reach, it is absolutely necessary to disable 2-Auth-Factor tokens to go to

State
○ New (Open)

Type
Authentication

New
New bugs must first be triaged by the Team they are reported to - understood, validated, and prioritized - before moving forward.

Please be patient during this process as it may take several days.

Triaged

Closed

Public

Participants

zero
Bug reporter

voicemail as voicemails cannot be trusted currently.

zero posted a comment. 17 days ago

Hi there, just adding that a large majority of mobile operators are vulnerable, and whilst I am trying my best to disclose the issue about the bypass of 2FA to them best as I can, it is unlikely that this will be fixed within the next month. Please disable sending codes to voicemail as a complete mitigation to this attack.

Thanks

zero posted a comment. 15 days ago

After doing some research, I was able to talk to the people at Duosecurity and Authy who specialise in 2FA. When I first discovered that Yahoo sent 2FA tokens to voicemail, I was so certain that 2FA providers such as Duosecurity and Authy were also vulnerable. I was wrong. They didn't sent 2FA tokens to voicemail. This is how they mitigated the issue:

- Requirement of some sort of user interaction before PIN/2FA token is issued via voice
- Leave a blank message in Voicemail instead of a pin
- Require a user interaction as a form of validation (2FA Call -> Told to press the number "x" -

All three of the methods listed above would be suitable to mitigate against this vulnerability.

zero posted a comment. 13 days ago

Hi there,

I have disclosed the bug to Optus (Telco) on the 2nd of May. In accordance with Google's vulnerability disclosure suggestions, the bug related to the telco's as well as the disclosure stating the possibility of bypassing 2FA will be disclosed publicly within 7 days.

I hope that Optus fixes the issue within 7 days, so that when we publicly disclose, Australian's are safe from the 2FA bypass I disclosed to you. However, if Optus does not fix this issue within due time, a public disclosure with the details of bypassing 2FA auth will be released.

From further research, I believe that the voicemail vulnerability is actively known and exploited in the wild, and hence believe it's necessary to continue with disclosure.

Hopefully, before the due date for disclosure, Yahoo receives this information.

zero posted a comment. 4 days ago

A public disclosure of this issue is bound to occur sometime tomorrow (Wednesday 13th May).

LinkedIn and Facebook have disabled the phone calling option temporarily, until a better fix is deployed. I highly recommend the same to secure your Australian users from the 2FA bypass.

Add a comment...

Write Preview Parsed with Markdown

Drag & drop or select more files from your computer (max. 10MB per file)

Post