Gmail by Google

Shubham Shah <@gmail.com>

Bypassing 2-Factor-Authentication via Voicemail Exploitation

5 messages

Shubham Shah <@gmail.com> Wed, Apr 30, 2014 at 1:27 AM
To: security@authy.com

To Authy,

Recently, I have found a number of 2-Faction-Authentication bypasses in multiple web applications. Whilst these major web applications from companies including Google, LinkedIn and Yahoo have not patched these 2FA vulnerabilities - I am sending this email to you as a vendor of such services so that you are also aware, and can deploy a fix.

I graciously ask you that your company does not make any of these issues public until further notice, and until other companies have had the chance to fix their 2FA systems.

The general method of exploiting 2FA has been documented below.

Please get back to me on whether or not Authy is indeed vulnerable to these attacks, and if Authy is planning to schedule a fix for it.

Thanks,
Shubham

===

Bypassing 2-Factor-Authentication via Voicemail

Assumptions/Pre-requisites for the attack to take place:
- The attacker has the victims mobile number (attached to "x" website)
- The attacker has the victims "x" websites email and password
- The attacker must have a spoofcard / Caller ID spoofer (e.g. Spoofcard.com works for this)

1. Attacker logs into the "x" websites account of the victim via any of "x" websites authentication flows. E.g. https://accounts.website.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 victim will instantly receive a text message on their phone but will not be alerted by this as they are already on the phone with attacker - however the attacker must quickly choose the 2FA option to call the victims phone.

3. Since the attacker is on the phone with the victim, the 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 bypass.

4. In Australia, the service provider (Optus) has 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

5. In the Spoofcard panel, I would merely spoof my victims mobile number, and call Optus's voicemail number (+61411000321)

6. Due to the spoof, Optus 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)

The only way I see this vulnerability/exploit being mitigated is by configuring the 2FA 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.

Shubham Shah <@gmail.com> Wed, Apr 30, 2014 at 2:10 PM
To: security@authy.com

I have just confirmed that this exploit works on Coinbase and that it affects the following providers in Australia:

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

Please get back to me ASAP.

[Quoted text hidden]

Daniel Palacio <d@authy.com> Thu, May 1, 2014 at 3:07 AM
To: Shubham Shah <@gmail.com>
Cc: security@authy.com

Hi Shubham,

Thanks a lot for contacting us. We've been aware of this attacks for a long time. We aren't vulnerable, since our calls are interactive. What this means is the user is required to press 1, and then the computer reads the token out loud. If the call goes to voice mail the only recorded part is this:

"Hi this is coinbase, if you were expecting this call please press 1".

That means the token is never disclosed on Voicemail. Let me know if this makes sense.

Daniel Palacio Founder, Authy Inc.
Skype: danipal
Call us: 1-855-687-2884
Follow-us: @authy

[Quoted text hidden]

Shubham Shah <@gmail.com> Thu, May 1, 2014 at 3:32 AM
To: Daniel Palacio <d@authy.com>

Brilliant!

Thanks for the extremely swift reply.

Both Authy and Duosecurity have some sort of an authentication process before issuing the OTP.

This is brilliant news, as it eliminates a large number of people from being vulnerable.

Sadly, the number of telco's vulnerable in Australia has now reached up to 12.

I would really appreciate if the disclosure I did to you remains confidential until further notice as I am still chasing up multiple vendors to fix this issue.

Cheers,
Shubham
[Quoted text hidden]

Daniel Palacio <d@authy.com> Thu, May 1, 2014 at 3:33 AM
To: Shubham Shah <@gmail.com>

No problem, we'll keep it private. Let us know when you disclose it.

Daniel Palacio Founder, Authy Inc.
Skype: danipal
Call us: 1-855-687-2884
Follow-us: @authy

[Quoted text hidden]