Re: Report a Security Vulnerability - Bypassing 2-Factor-Authentication on Facebook via Voicemail

Facebook Security <whitehat+xefcj3n.aeaq4unwhqrna@support.facebook.com> Tue, May 13, 2014 at 6:05 AM
Reply-To: Facebook Security <whitehat+xefcj3n.aeaq4unwhqrna@support.facebook.com>
To: @gmail.com

Hi Shubham,

We've temporarily disabled sending login approval codes via phone call while we investigate further. Our plan is to re-enable the system when we can prompt users for interaction as part of the phone call, which should prevent us from sending codes to voicemail boxes.

Thanks,

Neal
Security
Facebook

-----Original Message-----
From:
To:
Subject: Report a Security Vulnerability - Bypassing 2-Factor-Authentication on Facebook via Voicemail

Your Email Address:
Do you have technical details of a security vulnerability?: Yes
Vulnerability Type: Privacy / Authentication
Vulnerability Scope: Main Site (www.facebook.com)
Title: Bypassing 2-Factor-Authentication on Facebook via Voicemail
Product / URL: facebook.com
Description and Impact: It is possible to bypass the 2 Factor Authentication system on Facebook via voicemail hacking methodologies. Facebook does not handle the security of the pin correctly, and hence passes it on to an insecure endpoint which is somewhat always vulnerable. This vulnerability is going to be disclosed to the telco's in the following week (12th May 2014) and a publication may approach shortly after. Other affected vendors such as LinkedIn, have disabled 2FA via Phone Call, site-wide temporarily, to mitigate against this issue.
Reproduction Instructions / Proof of Concept: Assumptions/Pre-requisites for the attack to take place:
- The attacker has the victims mobile number (attached to Facebook)
- The attacker has the victims Facebook email and password
- The attacker must have a spoofcard / Caller ID spoofer (e.g. Spoofcard.com works for this)

1. Attacker logs into a Facebook account which has 2FA enabled

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 navigate to the option which allows for the sending of the 2FA code via a phone call, and then execute this option.

3. Since the attacker is on the phone with the victim, the Facebook's 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 Facebook 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.

Essentially, whilst it is definitely the Telco's problem. Not only does this mean that in the last four years (or more), people using an Optus based service in Australia (a large majority in Australia) were vulnerable to having their 2FA bypassed, it also means that it is very likely that many telco's in many countries are also very vulnerable to the same sort of attack.

I feel as if stating that it is purely a telco issue, is somewhat neglecting the fact that 2FA tokens don't have many good reasons to go to a persons voicemail. Additionally, by doing so, regardless that it is not Facebook's fault for 2FA being bypassable via an external vulnerability - the fact still remains that Facebook gives away this sensitive information to a potentially vulnerable end point.

Regardless of this, 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 Facebook 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" -> On press = verification, else = no verification).

Please do let me know what you think of this and if Facebook has any plans on mitigating against this. It's quite obvious that the issue is on the Telco's end due to insecure voicemail security - however it's not something which is in either Facebook's or my control and hence leaves 2FA vulnerable to some extent to such attacks.

2FA is absolutely useless to all Australian's who have linked their Optus number with Facebook, and has been useless for the last four years at the very minimum (assuming that others have known about the flaw in Optus voicemail security).
Is this bug public or known by third parties?: No
Can you reproduce this issue every time?: Yes
How did you find this bug?: Manually / Other

-----End Original Message-----