Shubham Shah <@gmail.com>

Bypassing 2-Factor-Authentication via Voicemail Exploitation

3 messages

Shubham Shah <@gmail.com> Wed, Apr 30, 2014 at 11:13 PM
To: security@duosecurity.com

To Duosecurity,

The PGP key is referenced to the incorrect location on your security page, and it shows up invalid on my end - hence I have had to send this email in plain text (sorry).

Recently, I have found a number of 2-Faction-Authentication bypasses in multiple web applications. Whilst these major web applications/services from companies including Google, LinkedIn, Yahoo and your competitor Authy 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 Duosecurity is indeed vulnerable to these attacks, and if Duosecurity 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.

This exploit works on 85% of the mobile networks in Australia and New Zealand. Whilst some will argue that the fault is of the service providers voicemail system (it largely is their fault), but it is unlikely that voicemail hacking will cease within the next few weeks or months and hence a mitigation technique on your end would be by ensuring no security tokens for 2FA go to voicemail.

Please do not disclose this issue with anyone as major voicemail providers are still vulnerable and by disclosure, people will not only be at risk of 2FA token stealing, but also by many malicious attackers sniffing voicemails for other purposes.

Thanks again,
Shubham Shah (we talked on twitter earlier @infosec_au)

Zach Lanier <zach@duosecurity.com> Wed, Apr 30, 2014 at 11:34 PM
To: Shubham Shah <@gmail.com>
Cc: security <security@duosecurity.com>

Shubham,

Thanks for your email. (We'll get the correct/updated PGP key on our site soon; no worries about plaintext for now.)

Incidentally, ANI spoofing (caller ID / phone number ID) is a pretty old trick -- academically speaking, glad to see it's still getting some mileage! The same voicemail-related security problems you've described, wherein the originating number would bypass PIN checks, have plagued *other* carriers around the globe:

http://www.theregister.co.uk/2014/04/24/voicemail_still_easy_to_hack/
http://www.moneytalksnews.com/2011/07/19/i-can-hack-into-your-voicemail/

As for Duo, we require user interaction for phone calls -- we don't leave the OTP in voicemail http://guide.duosecurity.com/other-phones & https://www.duosecurity.com/authentication-methods.

Good luck in your notification efforts with other vendors. Let us know if there's anything we can do to help.

Best regards,

Zach Lanier
--

Zach Lanier / Senior Security Researcher
zach@duosecurity.com
duosecurity.com

[Quoted text hidden]

Shubham Shah <@gmail.com> Wed, Apr 30, 2014 at 11:38 PM
To: Zach Lanier <zach@duosecurity.com>

Correct you are in saying that it's quite an old trick.

Congrats on being the first vendor that doesn't leave the OTP in voicemail. All other vendors that I have actually tested until now do so.

It's becoming quite alarming as now, the list of carriers has now tallied to be:

- 9 vulnerable to Caller ID/ANI spoofing
- 2 partially vulnerable to Caller ID/ANI spoofing

and

- 1 secure against such spoofing.

This is just in Australia.

Once again, your response was incredibly quick (unexpectedly), so I thank you for that.

Since I had no way of certainly checking that you indeed were not vulnerable, I felt that I'd send an email regardless.

Cheers,
Shubham