Gmail by Google

Shubham Shah <@gmail.com>

[7-8312000003367] Auth Problem in Gmail

3 messages

security@google.com <security@google.com> Wed, Apr 30, 2014 at 11:49 AM
To: @gmail.com

Thanks for the vulnerability report.

This email confirms we've received your message. We'll investigate and get back to you once we've got an update.

Cheers,

Google Security Bot

Report Details

Email Subject: [7-8312000003367] Auth Problem in Gmail

Category: Auth Problem

Product: Gmail

Cid: 7-8312000003367

Hi there, I have sent two emails to Google, the first accidentally being anonymous, and the second one to security@google.com in which I have received no reply. Just in case, I thought I would re submit with some added details - it is now an urgent matter as so many telco's have been confirmed as vulnerable.

In the last 24 hours, I have identified the following Australian telco's to be vulnerable to the voicemail trick:

Optus, Optus Business, Amaysim, Vodafone, TPG, Vaya, LiveConnected, Crazy Johns Mobile

Thanks

RL: 9rde7y8r9enp8r4xprtkiphi

Steps to reproduce the vulnerability:

Bypassing 2-Factor-Authentication via Voicemail

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

1. Attacker logs into the Google account of the victim via any of Google's authentication flows. E.g. https://accounts.google.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 click "Problems receiving your code?" and then continue to check "Call your primary phone:" - then press "Use this method".

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

In what Browser/OS/Platform/Version?
N/A

Additional details:
To test realistically, I attached my brothers phone to my Google account and enabled 2-factor-authentication. When he was at work, I executed the above method - with success.

Mitigation of this vulnerability is completely possible via disabling the feature that 2FA codes go to voicemail.

---

security@google.com <security@google.com> Thu, May 1, 2014 at 6:32 AM
To: @gmail.com

Hey,

Thanks for your bug report. We've taken a look at your submission and can confirm this is not a security vulnerability in a Google product. The attack presupposes a compromised password, and the actual vulnerability appears to lie in the fact that the Telcos provide inadequate protection of their voicemail system. Please report this to the telcos directly.

Regards,
Jeremy

Shubham Shah <@gmail.com> Sat, May 3, 2014 at 1:26 AM
To: "security@google.com" <security@google.com>

Hey Jeremy,

I completely understand and am chasing the Telco's at the moment as I disclose these vulnerabilities.

Regardless of pin protection, a large majority of telco's in Australia and UK require only a 4 digit pin with no lockouts. Essentially, using a VoIP service and some scripts on Asterisk AGI (http://www.voip-info.org/wiki/view/Asterisk+AGI) , it would be possible to break into a voicemail account within a day (concurrent instances of pin guessing).

Essentially, whilst you are right in saying that 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 Google's fault for 2FA being bypassable via an external vulnerability - the fact still remains that Google 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 Google 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 Google 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 Google'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 Google, 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).

Thanks,
Shubham

[Quoted text hidden]

[7-8312000003367] Auth Problem in Gmail

2 messages

security@google.com <security@google.com> Tue, May 6, 2014 at 2:41 AM
To: @gmail.com

Hi,

Thanks for explaining the potential scope of this issue.

Since it isn't technically a vulnerability in our 2SV system, I'm not sure if there's much we can do to mitigate this, but I've filed a bug a will ask the team to take a look.

Regards,
Jeremy, Google Security Team

Shubham Shah <@gmail.com> Tue, May 13, 2014 at 6:25 PM
To: "security@google.com" <security@google.com>

Hi there,

That's fine,

LinkedIn and Facebook have temporarily disabled 2FA via Phone Verification until further notice.

Their mitigation strategy as far as I know, is something like this:

- Disable phone verification temporarily
- Remodel 2FA service to use user interaction instead of pins, when through the phone call service (e.g. press 4842 when you get called)
- Enable the newer 2FA Phone Verification Service

Thanks,
Shubham

[Quoted text hidden]