

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF
CALIFORNIA

Case #: 4:19-cv-07123-PJH

Plntf Exhibit No. PTX-0932

Date Admitted: _____

By: _____

Kelly Collins, Deputy Clerk

From: Brendon Tiszka [/O=THEFACEBOOK/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=BRENDONTSEA]
Sent: 5/2/2019 9:42:19 PM
To: Brendon Tiszka [REDACTED@fb.com]; Drew Robinson [REDACTED@fb.com]
Subject: Message summary [{"otherUserFbId":100016050738937,"threadFbId":null}]
Attachments: sticker.png

Brendon Tiszka (5/02/2019 18:45:25 PDT):

>Hey Drew! We received a ping from whatsapp about this task T34775320. We're not sure if this is a legit vulnerability, but looking at the victim's adb logs, it seems that the service is being stopped P63566079 logs(https://our.intern.facebook.com/intern/tasks/view_inline_attachment/?attachment_id=690138184733755&fbid=472814263202094). We're having trouble reversing the 162 byte elf file that is dropped on the device -- would you be a good poc for this?

Brendon Tiszka (5/02/2019 18:51:08 PDT):

>@notify

Andrew Steven Robinson (5/02/2019 19:18:59 PDT):

>Yes I can look at that

Andrew Steven Robinson (5/02/2019 19:19:24 PDT):

>Do you need it tonight? If not I can take a look first thing tomorrow.

Andrew Steven Robinson (5/02/2019 19:19:44 PDT):

>162 bytes seems to small to be an entire elf though

Brendon Tiszka (5/02/2019 19:19:56 PDT):

>Yeah it does, I've started looking at it and it seems like valid arm

Brendon Tiszka (5/02/2019 19:20:11 PDT):

>That was a reply to the 162 bytes response

Andrew Steven Robinson (5/02/2019 19:20:41 PDT):

>Let me go get my laptop.

Brendon Tiszka (5/02/2019 19:22:02 PDT):

>Context: This might be a live whatsapp zero day but we aren't sure. I'm starting to dig into the voip code where the vulnerability would be.

>

>We have the payload here [https://phabricator.intern.facebook.com/P63568381\\$20](https://phabricator.intern.facebook.com/P63568381$20)

Andrew Steven Robinson (5/02/2019 19:26:03 PDT):

>reading backlog in the chat you added me to

Andrew Steven Robinson (5/02/2019 19:40:24 PDT):

>yea this isn't a valid ELF

Andrew Steven Robinson (5/02/2019 19:40:32 PDT):

>For one its missing the endian specification

Andrew Steven Robinson (5/02/2019 19:41:04 PDT):

>let me double check the commands being used to construct it and make sure I didn't make a mistake somewhere

Brendon Tiszka (5/02/2019 19:41:21 PDT):

>That's what we were getting, but were curious if it was obfuscated in some way. There is valid arm in there so I thought I would check with you

Andrew Steven Robinson (5/02/2019 19:57:44 PDT):

>ah I see, I've got it properly disassembled now

Andrew Steven Robinson (5/02/2019 20:35:03 PDT):

>I'm not 100% sure as I don't have access to the device I would need to verify this, but so far it looks like it opens a socket and reads/writes the socket.

Andrew Steven Robinson (5/02/2019 20:35:19 PDT):

>trying to figure out more details around the socket specifically as that part doesn't make much sense right now

Brendon Tiszka (5/02/2019 20:52:33 PDT):

>Awesome thanks! Is there an IP address in there that it is reaching out to?



Andrew Steven Robinson (5/02/2019 20:53:31 PDT):
>Yea I'm looking to see if I can find a valid sockaddr struct now

Andrew Steven Robinson (5/02/2019 21:00:48 PDT):
>I'm not seeing any valid sockaddr structs

Andrew Steven Robinson (5/02/2019 21:00:59 PDT):
>even if I did there aren't any connect or similar syscalls

Brendon Tiszka (5/02/2019 21:09:36 PDT):
>Great thanks! I think this is enough info for tonight, the rest can wait until morning in my opinion

Brendon Tiszka (5/02/2019 21:09:51 PDT):
>We are trying to reproduce now

Andrew Steven Robinson (5/02/2019 21:10:57 PDT):
>ok

Brendon Tiszka (5/02/2019 21:13:10 PDT):
>Thanks for looking at this :). From what I can tell the binary is outputting another binary (in the shell command) then executing that with hex arguments

Brendon Tiszka (5/02/2019 21:13:36 PDT):
>#thanks for helping reverse engineer an elf file that was potentially used in a whatsapp exploit
T34775320

Andrew Steven Robinson (5/02/2019 21:23:03 PDT):
>> Thanks for looking at this ☺. From what I can tell the binary is outputting another binary (in the shell command) then executing that with hex arguments
>yea so it writes the ELF to /data/data/com.whatsapp/files/t, with one noticable thing in that it writes the path "/data/data/com.whatsapp/files/tz" to the end of the elf.
>That get's chmod 777, and run where its supposed to pipe the output to the same
/data/data/com.whatsapp/files/tz path, but I don't see anything in this that would output anything to stdout, stderr, etc.

Andrew Steven Robinson (5/02/2019 21:23:10 PDT):
>Feels incomplete

Brendon Tiszka (5/02/2019 21:25:06 PDT):
>Do you mind if I post these updates in the chat?

Andrew Steven Robinson (5/02/2019 21:26:08 PDT):
>yea that's fine

Andrew Steven Robinson (5/02/2019 21:26:41 PDT):
>I'll double check with someone who knows ARM shellcode a lot better than I do tomorrow as well they may see something I missed.

Andrew Steven Robinson (5/02/2019 21:27:21 PDT):
>*Android ARM shellcode at that

Andrew Steven Robinson (5/02/2019 21:28:48 PDT):
>oh wait shit, there is a connect()

Andrew Steven Robinson (5/02/2019 21:28:54 PDT):
>I misread an add as a mov

Brendon Tiszka (5/02/2019 21:29:01 PDT):
>No worries!

Brendon Tiszka (5/02/2019 21:29:41 PDT):
>I'll just keep it succinct for now -- the elf file that is dropped appears to be an arm executable that opens a socket then reads/writes to that socket. We'll continue reversing tomorrow if anything comes up with the reproduction.

Brendon Tiszka (5/02/2019 21:30:07 PDT):
>We don't now if it this is a legit exploit or not

Andrew Steven Robinson (5/02/2019 21:30:12 PDT):

shared: sticker.png

Brendon Tiszka (5/02/2019 21:30:18 PDT):
>So we might not need to continue reversing tomorrow

Andrew Steven Robinson (5/02/2019 21:31:17 PDT):

>When you guys aren't so busy I'd like someone to sit down and explain this stanza stuff to me. this is the second time I've worked on WA stuff and I've still go no idea what they are or how we get the telem

Andrew Steven Robinson (5/02/2019 21:40:36 PDT):
[REDACTED] there's your IP address

Brendon Tiszka (5/02/2019 21:41:13 PDT):
>Can you post that in the chat? Andrey just asked

Andrew Steven Robinson (5/02/2019 21:41:15 PDT):
[REDACTED]

Andrew Steven Robinson (5/02/2019 21:41:15 PDT):
>hea

Andrew Steven Robinson (5/02/2019 21:41:17 PDT):
>*yea

Brendon Tiszka (5/02/2019 21:41:20 PDT):
>Thanks :)

Brendon Tiszka (5/02/2019 21:42:19 PDT):
>Thanks again!