بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

ارزیابی امنیتی نرم‌افزار متن باز Jitsi

گزارش ارزیابی

فهرست مطالب

۱ هدف

هدف از این ارزیابی موارد زیر است:

- ✓ استخراج تعاملات مشکوک این نرم‌افزار با خارج از سرور
- ✓ بررسی آسیب پذیری های برنامه های Client
- ✓ بررسی آخرین آسیب پذیریهای امنیتی و تاثیر آن بر امنیت جامعه‌ی بهره‌برداران
- ✓ مستندسازی پیکربندی امن و راهنمای راهبری و کاربری امن سامانه

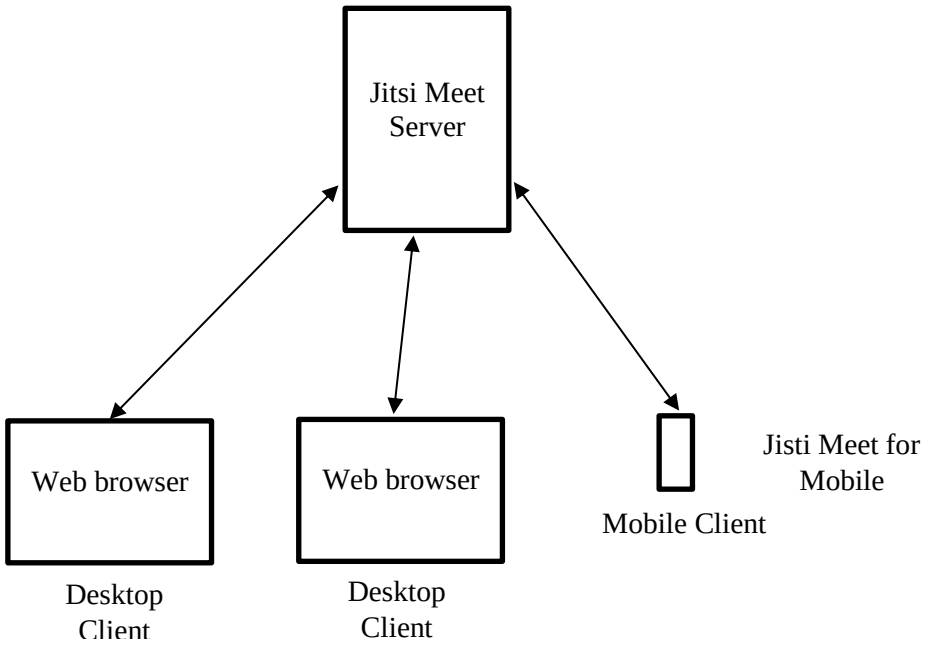
۲ معرفی سامانه

Jitsi یک راهکار ویدئوکنفرانس کاملاً رایگان و متن‌باز است. از ویژگی‌های امنیتی آن می‌توان به رمزنگاری سرتاسری در جلسات P2P (دو کاربره) و رمزنگاری بین کلاینت و سرور در جلسات چندکاربره اشاره کرد.

اکوسیستم Jitsi از اجزای مختلفی تشکیل شده است. Jitsi Meet Server سرور مورد استفاده در برگزاری جلسات است. کلاینت‌ها از طریق مرورگر وب با سرور ارتباط برقرار می‌کنند. محتوای چندرسانه‌ای نیز از طریق WebRTC به طور مستقیم بین کلاینت‌ها ارسال می‌شود. برای موبایل نیز از اپلیکیشن‌های Jitsi ویژه اندروید و iOS استفاده می‌شود. در جلسات چندنفره از یک مسیریاب ویدئو[1] (SFU[2]) به نام Jitsi Videobridge استفاده می‌شود که وظیفه انتقال محتوای ویدئویی را بین کلاینت‌ها به عهده دارد.

معماری آن به طور کلی به شکل زیر است (Videobridge نیز جزئی از Meet Server است):

[1] Video router
[2] Single Forwarding Unit



البته می‌توان بدون استفاده از سرور اصلی این نرم‌افزار با استفاده از یک سرور hosted (https://meet.jit.si) نیز جلسات را برگزار کرد.

۲-۱ روش فعالیت برنامه jitsi

برنامه jitsi به دو صورت می تواند فعالیت کند:

۲-۱-۱ peer-to-peer(P2P)

این روش تنها در ارتباطات دو نفره امکان پذیر است و در این حالت رمزگذاری به صورت end-to-end است و خود سرور میزبان هم از محتوای بسته های ارسالی باخبر نمی شود.

روش رمزنگاری end-to-end به صورت DTLS-SRTP و مطابق استاندارد RFC-5764 و RFC-5763 پیاده سازی شده است.

اطلاعات بیشتر در مورد این روش و نحوه چگونگی آن در وب سایت زیر مورد بررسی قرار گرفته است.

https://tools.ietf.org/html/rfc5763

به طور خلاصه در این روش یک master key بین دو کاربر از طریق کانالی جز ارتباط فعلی رد و بدل می شود به طور مثال master key به صورت تماس تلفنی و یا پیام در یکی از پیام رسان ها به طرف مقابل ارسال می شود و از روی آن کلید session key ها تولید می شود و تا هر session با کلید خودش امن شود .

این master key با password که برای پیوستن به اتاق گفت و گو استفاده می شود متفاوت است.

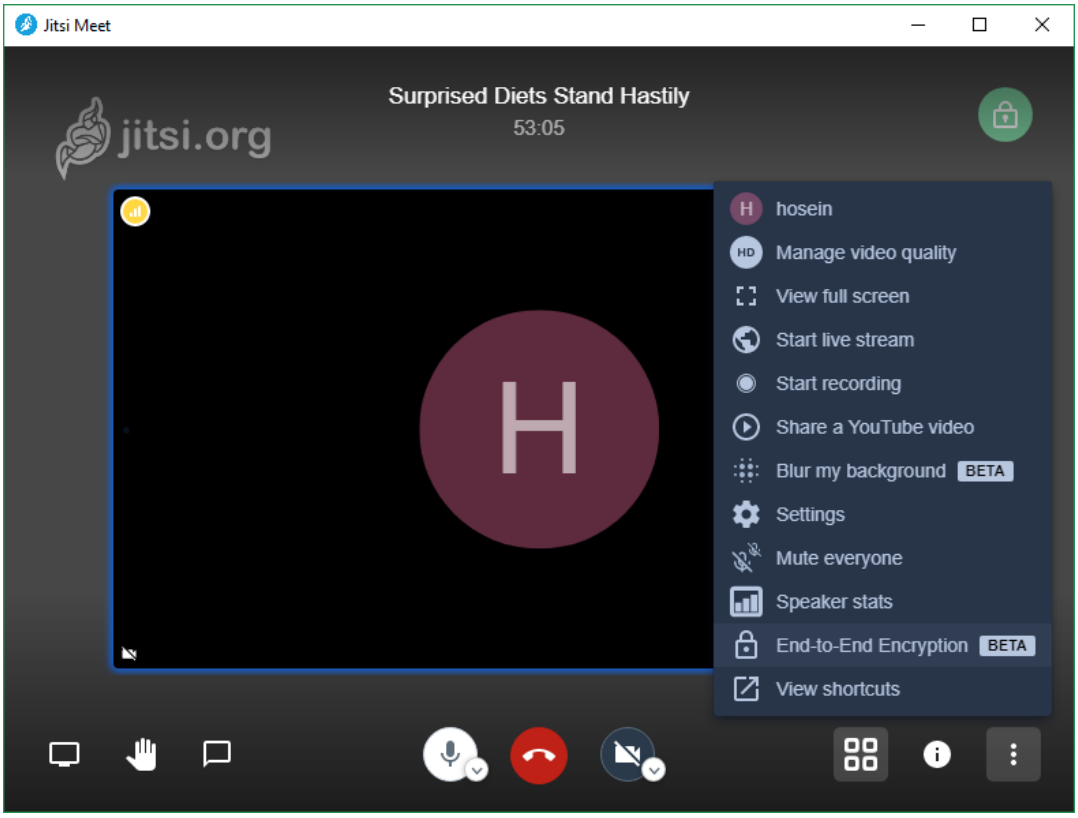
لازم به ذکر است این مدل ارتباط P2P تنها بر روی سرور خود Jitsi در حال حاضر وجود دارد و با آدرس زیر می توان این ارتباط را برقرار کرد

https://meet.jit.si/

امکان استفاده از سرور اختصاصی JITSI خود مشتری برای رمز نگاری end-to-end هنوز فراهم نشده است.

همچنین این قابلیت هنوز به صورت آزمایشی برای Jitsi در حال اجرا است و در حال تنظیم این سند صرفا از روی برنامه Jitsi Mett Electro، Desktop این امکان فراهم است در بررسی مجدد https://meet.jit.si/ دیگر امکان برقرار کردن ارتباط به صورت end to end برداشته شده است در صورتی که تا پیش از این این قابلیت در سایت هم مشاهده می شد.

همان طور که در تصویر زیر مشاهده می شود امکان برقراری ارتباط به صورت end to end در منوی تنظیمات به صورت beta قرار داشت که کاربر با مشخص کردن master key و ارسال آن به صورت دستی برای طرف مقابل تنها به صورت کنفرانس دو نفره قادر به برقراری ارتباط end to end بود. مشخص نیست این امکان چه زمانی بر روی سرور خود jitsi و همچنین سرور های jitsi video bridge فراهم شود.

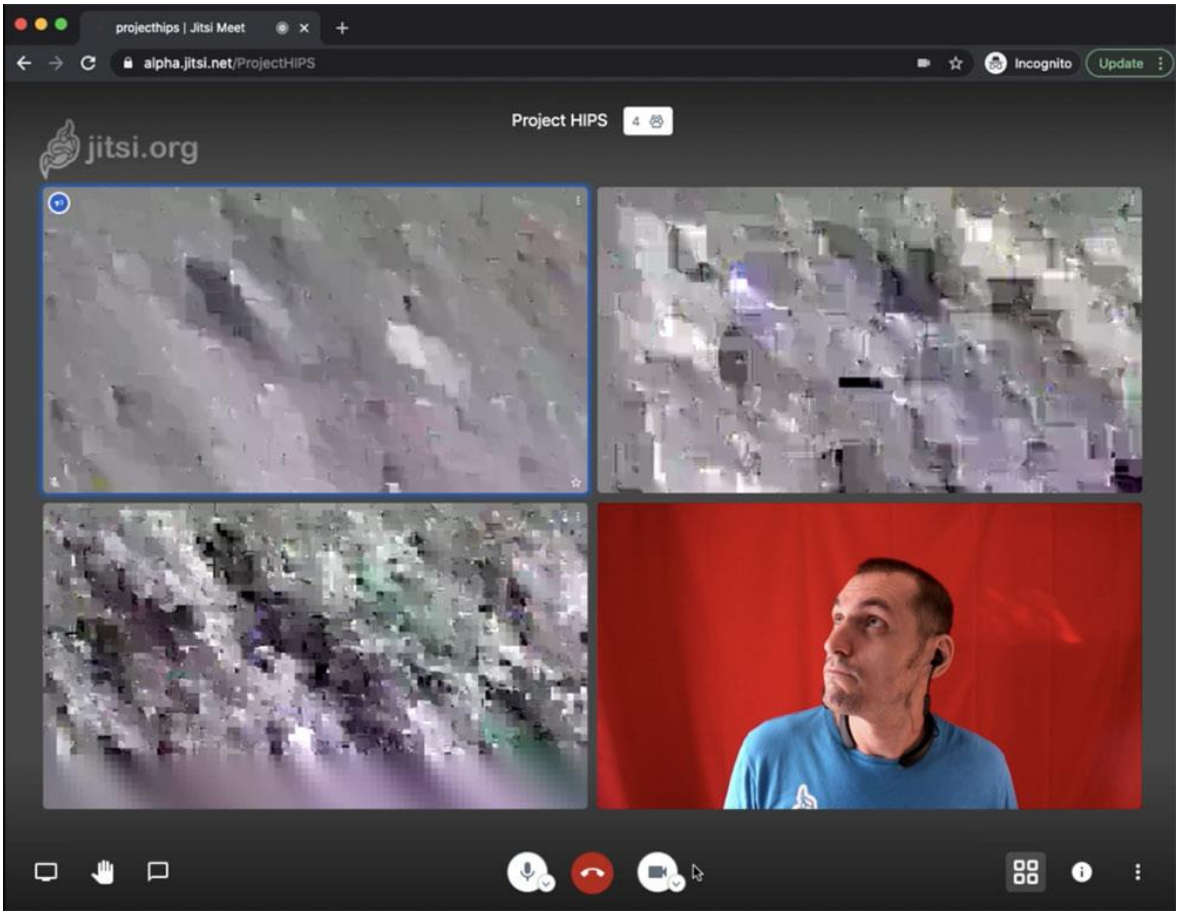


شکل ۱: برقراری ارتباط به صورت end to end

به صورت کلی همان طور که در شکل بالا مشاهده می شود از بخش تنظیمات کناری jitsi با انتخاب گزینه End to End encryption می توان کلید master key تعیین کرد. بعد از انتخاب کلمه ای عبور برای master key ، URL به شکل زیر در می آید .

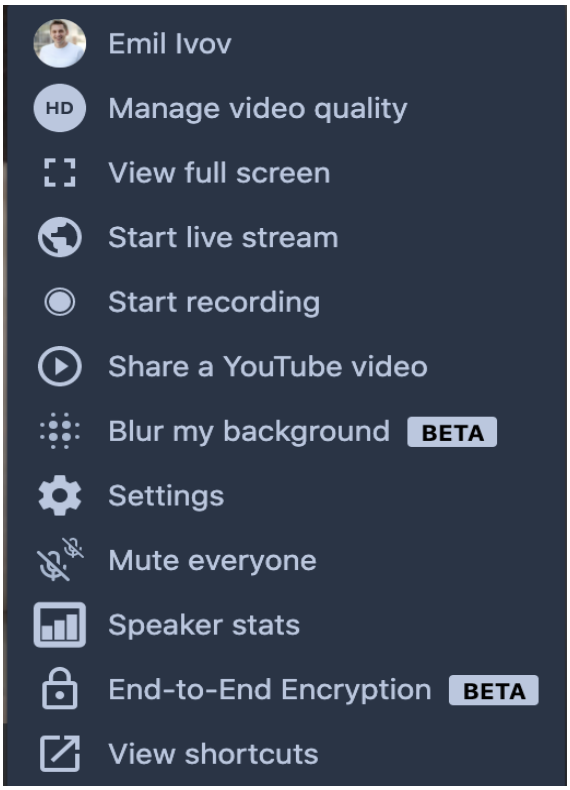
https://meet.jit.si/SurprisedDietsStandHastily#e2eekey=foo

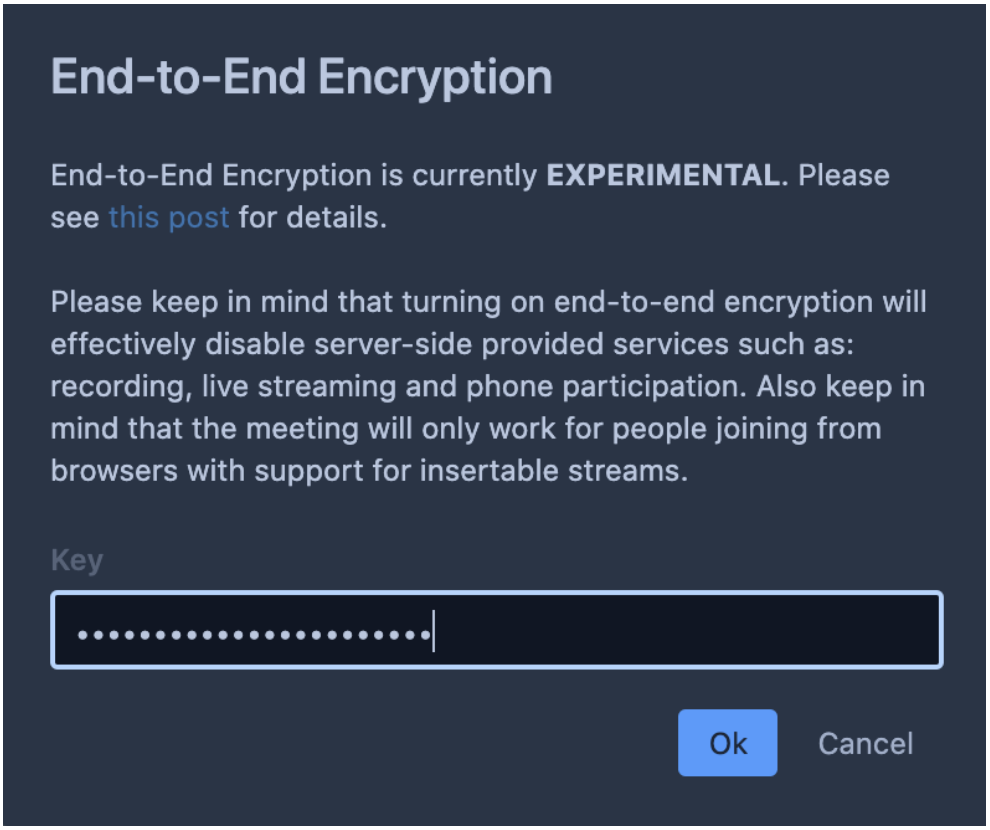
در صورتی که قست master key در URL وارد نشود صدا و تصویر انتقال پیدا می کند ولی رمز شده است و تصویری شبیه تصویر زیر مشاهده می شود.



شکل ۲: انتقال صدا و تصویر به صورت رمز شده

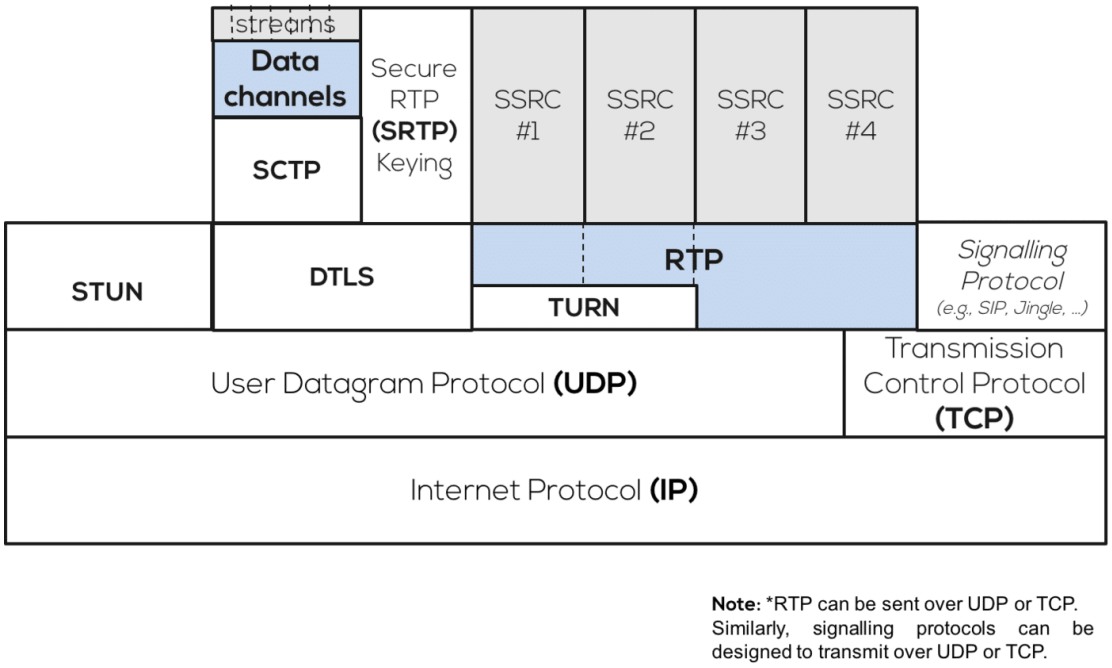
در شکل زیر نحوه ایجاد این master key را می بینید.





شکل ۳: نحوه ایجاد master key

ساختار رمز کردن بسته های WebRTC در شکل زیر مشاهده می شود .



شکل ۴ : ساختار رمز کردن بسته های WebRTC

همان طور که مشاهده می شود پروتکل SRTP قسمت payload (داده های اصلی) بسته ها را که حاوی همان داده های audio , video هستند را رمز می کند تا بسته ها به جز برای طرف مقابل قابل شنود نباشند.

رمز نگاری استفاده شده برای این منظور AES است که تا این لحظه امن تلقی می شود.

WebRTC که پروتکلی برای ارتباط زمان-حقیقی (real time) و انتقال audio , video است با استفاده از DTLS-SRTP از موارد زیر بهره میبرد:

- Confidentiality : به وسیله رمزکردن payload RTP
- Message authentication
- Integrity
- Replay attack protection

Key management یکی از سختی های SRTP است که به وسیله پیاده سازی DTLS-SRTP که یک روش مقبول است و امنیت آن تا این لحظه در مخاطره نیست انجام می شود.

همچنین این برنامه از DTLS v 1.2 استفاده می کند که نسخه با امنیت بهتری است که از رمزنگاری AES128 و تابع درهمریز SHA256 و زنجیرسازی داده ها به صورت GCM بهره می برد.

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

برای اطلاعات بیشتر می توان به وب سایت زیر مراجعه کرد

https://tools.ietf.org/html/draft-ietf-rtcweb-security-arch-20

۲-۱-۲ Jitsi Video Bridge (JVB)

در این روش که برای مکالمات بیشتر از دو نفر انجام می شود از همان روش قبل یعنی DTLS-SRTP استفاده می شود ولی این ارتباط بین هر کاربر و سرور JITSI است.

در واقع به دلیل مشکلات مقیاسی نیاز به یک third party برای ارتباط بیشتر از دو نفر داریم.

ارتباط تا سرور JITSI به همان شکل که در روش اول توضیح داده شد امن است اما در سرور محتوای بسته ها رمز گشایی می شود و در ادامه مسیر تا رسیدن به نفر بعدی با رمز جدیدی دوباره رمز می شود.

در این حالت در خود سرور تنها امکان شنود مکالمات وجود دارد.

لازم به ذکر است کلیه اطلاعات فوق با بررسی کد های باز برنامه jitsi مطابقت داشته است و تمام مطالب با بررسی مقالات آورده شده در این گزارش و بررسی کد های باز jitsi نوشته شده است.

۲-۲ بررسی برنامه های Client

برنامه jitsi در نسخه های مختلفی بر روی client ها می تواند مورد استفاده قرار بگیرد.

نسخه Desktop این برنامه با نام jitsi-meet-electron و نسخه اندوید و IOS برنامه با نام jitsi meet عرضه شده است. هر دوی این برنامه ها متن باز هستند.

در بررسی های انجام شده تمام clientها هیچ ارتباطی جز با سرور اصلی که برای برنامه تعریف می شود ندارند.

تمام اتصالات برنامه ها خارج از ارتباط Local host و ip server نیست.

Protocol	Local Address	Remot...	State
TCP	127.0.0.1:11459	0.0.0.0:0	LISTENING
UDP	0.0.0.0:6768	*:*	
UDP	0.0.0.0:20014	*:*	
UDPV6	[0:0:0:0:0:0:0:0]:6768	*:*	
UDPV6	[0:0:0:0:0:0:0:0]:20014	*:*	

تمام این کتابخانه ها به جز یکی کتابخانه های ویندوزی هستند که این برنامه از آنها استفاده میکند.

در ادامه به بررسی موارد مورد استفاده jitsi.exe می پردازیم.

در زیر dll های مربوط به خود برنامه را آورده ایم تا از لحاظ DLL Injection بررسی شوند.

Name	Description	Company Name	Path	ASLR	Image Type
locale.nls			C:\Windows\System32\locale.nls	n/a	n/a
Jitsi.exe	Jitsi	jitsi.org	C:\Program Files\Jitsi\Jitsi.exe		64-bit
apphelp.dll	Application Compatibility Client Library	Microsoft Corporation	C:\Windows\System32\apphelp.dll	ASLR	64-bit
profapi.dll	User Profile Basic API	Microsoft Corporation	C:\Windows\System32\profapi.dll	ASLR	64-bit
powrprof.dll	Power Profile Helper DLL	Microsoft Corporation	C:\Windows\System32\powrprof.dll	ASLR	64-bit
fltLib.dll	Filter Library	Microsoft Corporation	C:\Windows\System32\fltLib.dll	ASLR	64-bit
kernel.appcore.dll	AppModel API Host	Microsoft Corporation	C:\Windows\System32\kernel.appcore.dll	ASLR	64-bit
KernelBase.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\KernelBase.dll	ASLR	64-bit
win32u.dll	Win32u	Microsoft Corporation	C:\Windows\System32\win32u.dll	ASLR	64-bit
windows.storage.dll	Microsoft WinRT Storage API	Microsoft Corporation	C:\Windows\System32\windows.storage.dll	ASLR	64-bit
cfgmgr32.dll	Configuration Manager DLL	Microsoft Corporation	C:\Windows\System32\cfgmgr32.dll	ASLR	64-bit
msvcp_win.dll	Microsoft® C Runtime Library	Microsoft Corporation	C:\Windows\System32\msvcp_win.dll	ASLR	64-bit
gdi32full.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\System32\gdi32full.dll	ASLR	64-bit
bcryptprimitives.dll	Windows Cryptographic Primitives Library	Microsoft Corporation	C:\Windows\System32\bcryptprimitives.dll	ASLR	64-bit
ucrtbase.dll	Microsoft® C Runtime Library	Microsoft Corporation	C:\Windows\System32\ucrtbase.dll	ASLR	64-bit
msvcrt.dll	Windows NT CRT DLL	Microsoft Corporation	C:\Windows\System32\msvcrt.dll	ASLR	64-bit
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\System32\advapi32.dll	ASLR	64-bit
kernel32.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\kernel32.dll	ASLR	64-bit
shlwapi.dll	Shell Light-weight Utility Library	Microsoft Corporation	C:\Windows\System32\shlwapi.dll	ASLR	64-bit
combase.dll	Microsoft COM for Windows	Microsoft Corporation	C:\Windows\System32\combase.dll	ASLR	64-bit
sechost.dll	Host for SCM/SDDL/LSA Lookup APIs	Microsoft Corporation	C:\Windows\System32\sechost.dll	ASLR	64-bit
imm32.dll	Multi-User Windows IMM32 API Client DLL	Microsoft Corporation	C:\Windows\System32\imm32.dll	ASLR	64-bit
shell32.dll	Windows Shell Common Dll	Microsoft Corporation	C:\Windows\System32\shell32.dll	ASLR	64-bit
user32.dll	Multi-User Windows USER API Client DLL	Microsoft Corporation	C:\Windows\System32\user32.dll	ASLR	64-bit
psapi.dll	Process Status Helper	Microsoft Corporation	C:\Windows\System32\psapi.dll	ASLR	64-bit
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\System32\gdi32.dll	ASLR	64-bit
rpcrt4.dll	Remote Procedure Call Runtime	Microsoft Corporation	C:\Windows\System32\rpcrt4.dll	ASLR	64-bit
SHCore.dll	SHCORE	Microsoft Corporation	C:\Windows\System32\SHCore.dll	ASLR	64-bit
ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\Windows\System32\ntdll.dll	ASLR	64-bit

شکل ۵ : dll های مربوط به برنامه

در مورد احتمال حمله DLL Injection توسط دیگر پروسس ها به Jisti.exe باید گفت که با وجودی که این پروسس به طور کامل توسط لایه امنیتی ASLR محافظ نمی شود ولی به دلیل اینکه هسته این برنامه به زبان java نوشته شده است و همچنین در کد های این برنامه جایی برای buffer over flow پیدا نگردید احتمال وقوع این حمله و دسترسی به فضای حافظه برنامه وجود ندارد.

۳ فرضیات ارزیابی

در ارزیابی این سامانه فرض‌های زیر در نظر گرفته شده است:

- ✓ بهره‌برداران ممکن است از نسخه‌ی نصب شده در سایت meet,jit.se استفاده کرده یا ممکن است خود نسخه‌ی نصب شده در سرور اختصاصی خود را استفاده کنند.
- ✓ بهره‌برداران ممکن است از هر کدام از کلاینتهای وبی، اندرویدی یا ios و ویندوزی این برنامه استفاده کنند.
- ✓ بهره‌برداران عمدتا از رایانه‌ها و گوشیهای شخصی و لزوما سازمانی برای اتصال به نشست‌ها و جلسات استفاده کنند.

۴ سناریوهای تهدید

در این بخش سناریوهای محتمل تهدید این برنامه برای مصارف سازمانهای داخلی آورده شده است.

۴-۱ شنود در حالت استفاده از نسخه‌ی نصب شده در سایت meet,jit.se

همان طور که در بخش معرفی توضیح داده شد به دلیل رمز نگاری end to end (که البته هنوز به صورت beta است و به صورت کامل در دست رس قرار نگرفته) امکان شنود اطلاعات در مکالمات دو نفره در صورت انتساب master key برای مکالمه وجود ندارد. اما در سایر مکالمات بسته های payload در سرور decrypt می شوند و محتوای آنها قابل شنود است.

در صورت راه افتادن رمزنگاری end to end تا زمانی که راهی برای شکست رمزنگاری ارتباط DTLS-SRTP کشف نشده باشد، شنود ارتباط end to end میان دو نفر امکان پذیر نیست.

اطلاعاتی نظیر زمان برگزاری جلسات و اینکه چه کسانی در جلسه هستند و با هم صحبت می کنند هنوز در ارتباط end to end هم قابل دستیابی برای تمام کسانی که بسته ها را شنود می کنند وجود دارد و تنها محتوای بسته ها رمز شده است.

۴-۲ شنود توسط مدیر سرور

ارتباط گروهی افراد توسط ادمین سرور jitsi یا کسی که دسترسی به سرور پیدا کرده است بصورت کامل قابل شنود است؛ چه سرور خود jitsi و چه سرور اختصاصی مشتری.

۴-۳ امکان شنود در حالت استفاده از گواهی SSL نامعتبر

استفاده از SSL معتبر و یا تونل ارتباطی (VPN) می تواند اطلاعات هدر های بسته های WebRTC (همان زمان تشکیل جلسات و افراد در جلسه) را برای شنود کننده ها به جز در درون خود سرور امن سازد. یعنی کسی که در بین راه بسته را می بیند دیگر اطلاعات درون webRTC header را نمی تواند استخراج نماید. در صورت عدم استفاده از SSL نیز همچنان محتوای بسته ها شامل audio , video قابل شنود برای افراد نیست و تنها در سرور اینکار قابل انجام است. البته توجه داشته باشید که استفاده از SSL وابستگی بسته های داده را به یکدیگر زیاد کرده و بدلیل عدم وجود ارسال های مجدد (retransmission) در ارتباطات زمان-حقیقی می تواند باعث پایین تر آمدن کیفیت ارتباط در صورت از دست رفتن برخی بسته ها شود.

۴-۴ ارتباط مشکوک سرور اختصاصی با مبادی بیرونی

از بررسی های انجام شده بر روی کد اجرا شده روی سرور اختصاصی خودمان ارتباطی مشکوک با خارج از سرور دیده نشد. همچنین به دلیل کد باز بودن برنامه چنین backdoorهایی در برنامه معمولا وجود ندارد چرا که چنین back doorهایی به دلیل کد باز بودن برنامه برای همه برنامه نویسان عیان می شود و باعث بی آبرویی آن تولید کننده است و کلا یکی از مزایای برنامه های کد باز همین است که هر کسی می توان بررسی نماید که back door در برنامه وجود دارد یا خیر. البته این موضوع به معنای عدم وجود آسیب پذیری های امنیتی در کد باز نیست، و لازم است پس از کشف شدن آسیب پذیری در کدهای مورد استفاده، وصله های امنیتی جهت رفع مشکل توسط شرکت تولید کننده ارائه شود.

۴-۵ نفوذ از طریق آسیب‌پذیریهای منشتر شده

بررسیهای ارزیاب نشان می‌دهد که Jitsi در مجموع دو CVE ثبت شده دارد:

- ✓ CVE-2020-1187 : آسیب‌پذیری از رده بحرانی و با امتیاز CVSSv3 = 9.8
- ✓ CVE-2017-5603 : آسیب‌پذیری از رده متوسط و با امتیاز CVSSv3 = 5.9

آسیب پذیری های شناخته شده در مورد این برنامه به سرعت Patch شده اند و ورژن فعلی برنامه آسیب پذیری شناخته شده ای ندارد.

۴-۶ امکان نفوذ به ارتباط end to end از طریق حدس کلمه master key

پیچیدگی رمز انتخاب شده در ارتباط End to End که به عنوان master key استفاده می شود صرفا اگر قابل حدس زدن نباشد کفایت می کند چرا که به وسیله یک کد JavaScript یک salt پیچیده به آن اضافه می شود و در نهایت در همان browser client کلید های session تولید می شود.

۴-۷ ازتباطات مشکوک client ها

در بررسی های انجام شده مشکلی در برنامه های کلاینت ها اندرویدی و ویندوزی دیده نشد و ارسالی به غیر از سرور اصلی ندارند.

۴-۸ امکان دسترسی به فضای حافظه برنامه های client توسط یک برنامه مخرب و شنود اطلاعات

در این بخش با بررسی حمله DLL Injection به process برنامه jitsi مشخص شد که این برنامه در مواجه با این حمله آسیب پذیر نیست.

۴-۹ آسیب‌پذیری‌های منتشر نشده

با توجه به اینکه امکان وجود آسیب‌پذیریهای منتشر نشده هست، مطابق توصیه سایت توسعه دهنده‌ی این نرم‌افزار بایستی این نرم‌افزار تحت کاربر root اجرا نشود.

۵ جمع‌بندی

با توجه به گستردگی استفاده از این نرم‌افزار و تعدد انتشارها و توسعه‌ها و نسخه‌های آن (حدود release ۷۰۰۰) این نرم‌افزار یکی از نرم‌افزارهای پر استفاده در زمینه‌ی ویدیو کنفرانس است. در استفاده از این برنامه بایستی به موارد زیر توجه ویژه داشت:

- ✓ مخفی کردن آدرس سرور از روشهای مانند روشها زیر می‌تواند در بالابردن امنیت کاربری آن کمک شایانی کند:
  - تغییر پورت پیش‌فرض ۴۴۳
  - تغییر banner و امضاء خاص این برنامه برای مخفی ماندن از اسکنرهای بین‌المللی
- ✓ سرور به روز باشد و آخرین به روز رسانی های امنیتی روی آن برقرار باشد
- ✓ سرور تست نفوذ پذیری امنیتی شود و از عدم داشتن آسیب پذیری امنیتی اطمینان حاصل شود
- ✓ هر کدام از برنامه های نصب شده روی سرور می تواند آسیب پذیری هایی داشته باشد و باعث دسترسی به سرور شوند لذا هر چه کمتر برنامه های اضافه و پورت های سرور باز باشند امکان و احتمال آسیب پذیری کمتر می شود.
- ✓ دسترسی SSH سرور به صورت public-private key باشد و کلید private نیز از روی سرور حذف شود.
- ✓ کاربر root حتما به صورت remote امکان دسترسی به سرور را نداشته باشد و محدود شود.
- ✓ برای استفاده و اجرای برنامه jitsi از کاربری جز root استفاده شود.
- ✓ عدم استفاده از نام room و کلمات عبور ساده
- ✓ بر روی سرور firewall UFW یا هر فایروال دیگری استفاده شود و امکان دسترسی به SSH یا دیگر دسترسی های admin را صرفا محدود به آدرس هایی خاص در شبکه کنند. برای مثال دسترسی به SSH تنها از طریق یک ip خاص صورت پذیرد.
- ✓ SSL به سه روش می تواند پیاده سازی شود:
  - Already Available certificate
  - Certificate from Lets Encrypt
  - Self-signed certificate

به ترتیب از بالا به پایین certificate ارائه شده برای SSL در موارد فوق اعتبار کمتری دارد

- ✓ باید از اعتبار certificate ارائه شده مطمئن بود و جز تست های سرور باید تست SSL هم قرار گیرد.

- ✓ پورت هایی که jitsi روی آنها فعالیت میکند پورت های 10000~20000 , 443 , 80 است که پورت 10000~20000 برای ارتباط WebRTC استفاده می شود. لذا با استفاده از فایروال باز هم میتوان مدیریت و مانیتورینگ بهتری روی این پورت ها انجام داد.
- ✓ عدم استفاده از نسخه‌ی نصب شده در سایت رسمی برنامه و نصب نسخه‌ی اختصاصی
- ✓ استفاده از قابلیت‌های هویت‌شناسی که در نرم‌افزار گنجانده شده است.
- ✓ در نهایت اگر امنیت سرور jitsi را حفظ نماییم و مورد آزمون نفوذ قرار گیرد می توان تا حد مورد قبولی از عدم شنود افراد غیر اطمینان حاصل کرد.