webinar please®

La Sécurité des Visioconférences, un monde idéal !

Bienvenue dans le Monde merveilleux de la Visioconférence et ses failles de sécurité ! Vous pensez que l'enjeu de la sécurité des webconférences se résume aux écoutes pirates ? Non, le problème est plus vaste et reste assez confidentiel.

En une phrase : les visioconférences peuvent exposer gravement la sécurité de vos postes et réseaux !

Qui m'écoute ?

Pour comprendre où se trouvent les failles de sécurité des visioconférences et webinars, il faut appréhender le fonctionnement de « WebRTC » (Web Real Time Communication)

WebRTC est un nouveau standard Web soutenu par W3C et IETF à l'initiative de Google. Il permet de commuter des ordinateurs entre eux au moyen de la technologie Peer to Peer.

Les communications audio-vidéo entre terminaux sont cryptés : SDP et DTLS sécurisent les données tandis que SRTP sécurise les échanges, selon les pratiques recommandées.

Mais lorsque les communications ne sont mal sécurisées, il est possible d'écouter les flux audio-vidéo. En plus de nombreuses solutions ne sécurisent pas convenablement l'identité du participant qu'un hacker peut usurper selon cette thèse de Polytechnique Catalogne (PDF).

C'est parce que tous les systèmes de visioconférence ne se valent pas, que l'espionnage de données ou autres informations est alors parfois possible.

On se souvient, en Novembre 2020, d'une conférence « confidentielle » de la Commission Européenne, à laquelle un journaliste accéda sur Zoom.

Mais retenons qu'un véritable pirate ne vous contactera pas pour signaler son méfait, et qu'il existe plusieurs méthodes, et failles de sécurité, connues et non connues...

webinar please®

Quels enjeux ?

Parmi les failles de sécurité des webinars, le plus troublant est que WebRTC fait l'inventaire de votre réseau pour accéder aux terminaux, derrière votre firewall.

Enorme ? Non, c'est la procédure standard, car l'inventaire des terminaux est nécessaire pour associer les terminaux dans un ou plusieurs réseaux sécurisés.

Concrètement, pour connecter trois postes en Peer to Peer lors d'une visioconférence, le système WebRTC (Teams, Zoom, Jitsi, etc) inventorie les informations des terminaux.

Pour contourner les firewalls, WebRTC attribue une adresse aux terminaux d'un réseau sécurisé. Ces procédures sont complexes et peu communiquées par les éditeurs.

Ces données permettent d'accéder aux postes du réseau sécurisé, elles transitent via un serveur dont vous ne connaissez pas l'emplacement, la sécurité et la législation applicable.

Bien que le cas soit fréquent, les éditeurs de visioconférence informent rarement leurs usagers que la technologie est opérée par des sous-traitants étrangers.

Le plus souvent, ces informations sont hors de votre contrôle. Vous ne disposez pas de l'inventaire des services de communication WebRTC (Turn, Stun, ICE pour « Établissement de Connectivité Interactive ») qui permettent aux terminaux de se connecter.

Cette complexité est un point faible pour la sécurité des visioconférences et webinars.

Par facilité, beaucoup d'éditeurs se disent conformes au RGDP. Mais c'est insuffisant, surtout lorsque le système affirme être conforme et sécurisé.

Quels risques réels ?

Vous doutez des informations de cet article ? Vous avez raison, il faut de preuves pour avérer cette affirmation : « des données peuvent être piratées ! »

D'abord précisons qu'un internaute qui participe à une visioconférence depuis son domicile, même équipé d'un VPN, peut exposer une IP publique, et faire l'objet d'attaques. Cela provient du fonctionnement standard du navigateur en présence de script malicieux.

Mais revenons à ICE (Établissement de Connectivité Interactive) qui permet de reconnaître les postes connectés à une visioconférence WebRTC.

Pour fonctionner ICE exploite la technologie Turn pour traverser les réseaux sécurisés afin de commuter les ordinateurs participant à une visioconférence, depuis un réseau protégé.

C'est ce que les ingénieurs réseaux nomment une « résolution NAT », qui permet d'accéder aux postes dans un réseau intranet.

Bien que des méthodes existent pour sécuriser le serveur Turn et les terminaux, les éditeurs ne sont guère bavards sur ce point.

Quels piratages récents ?

Déjà en 2014 les ingénieurs d'Ericsson étudiaient les défauts de sécurité du procédé Turn : « un attaquant qui est capable d'écouter un échange de messages entre un client et le serveur pour déterminer le mot de passe » Ce que confirmait Zataz, comme une faille impactant la sécurité des VPN.

Décembre 2018, durant la conférence SecureComm, étaient exposées les méthodes pour un « abus des navigateurs Web pour le stockage et la distribution de contenu caché »

Avril 2020, le Forum « Future of Internet » notait « Le problème de l'utilisation de WebRTC afin de cartographier la topologie intranet à partir d'un attaquant externe » et propose une analyse très documentée (PDF).

Juin 2020, un forum de sécurité faisait part de l'abus du service Turn de la société 8×8 éditeur américain de Jitsi, précisant que cet exploit « permet aux attaquants distants d'atteindre les services internes sur le serveur lui-même ainsi que sur le réseau interne AWS ».

Septembre 2021, RTSEC, expert en sécurité, annonce que les serveurs Turn de la société Slack (12 millions d'utilisateurs jour) ont pu être abusés pour accéder aux « services internes ».

La sécurité de WebRTC n'est donc pas une légende, c'est un sujet brûlant.

Quelle solution ?

Résumons. Ces problématiques de sécurité des visioconférences WebRTC peuvent exposer la sécurité des réseaux, des terminaux…

C'est pourquoi, sans conteste, une solution de visioconférence devrait pouvoir détailler ses des garanties fortes de sécurité.

Cela ne se discute plus, indépendamment du niveau de confidentialité des communications, la technologie de visioconférence WebRTC peut exposer la sécurité informatique.

Au-delà des procédures pour sécuriser les flux audio-vidéo et leur transport (SDP, DTLS, SRTP), les composants de communication (ICE, Stun, Turn), un terme s'impose pour garantir un haut niveau de sécurité : **« Architecture sécurisée de bout en bout »**.

La sécurisation de bout en bout, aussi nommée « e2ee » (End to End Encryption) a pour objectif de crypter tous les points d'échanges de l'architecture WebRTC : terminaux et serveurs afin de protéger vos ressources et vos communications.

La question centrale est donc « cette application de visioconférence est-elle cryptée de bout en bout ? ».

Mais soulignons aussi qu'une certification de sécurité valide les pratiques de développement et d'hébergement, sans faire l'inventaire des aléas hors périmètre… précision nécessaire.

webinar please®

Quel critère exiger ?

Le cryptage de bout en bout est un indicateur incontournable pour votre sécurité.

En Avril 2021, un guide de la fondation « Front Line Defenders » conclu que de nombreux systèmes de visioconférence ne sont pas encore cryptés de bout en bout.

Ce guide précise que Jitsi Meet y travaille (encore), tandis qu'avec Teams « une personne ayant accès à ces serveurs peut potentiellement intercepter vos messages ».

Et ce guide reste assez prudent sur d'autres solutions : « Nous n'avons pas inclus les outils tels que Zoom, Skype, Telegram, WhatsApp ... la marge de risque lors de leur utilisation est trop grande ».

Le cryptage de bout en bout est un critère exigible.

En France, les solutions logicielles WebinarPlease d'Empreinte.com, Tixeo, Rainbow d'Alcatel Lucent, sont cryptées de bout en bout, ouvrant la voie à des systèmes sécurisés.

Empreinte.com précise enfin ne pas installer de logiciel sur les terminaux afin de simplifier la vie des utilisateurs et DSI, complétant la citation de Tim Berners Lee « Le but ultime du Web est de soutenir et d'améliorer notre existence » pas de la compliquer...

Que vous soyez DSI ou internaute vous connaissez désormais la règle du jeu : une recherche exigeante et continue, une solution cryptée de bout en bout, ou une certaine incertitude...

C'est à vous de voir !

---

(1) https://www.journaldugeek.com/2011/06/15/google-webrtc-chat-video-audio-navigateur/
(2) https://www.w3.org/TR/webrtc/
(3) https://www.rfc-editor.org/rfc/rfc8835.html
(4) https://tools.ietf.org/id/draft-nandakumar-rtcweb-sdp-01.html
(5) https://fr.wikipedia.org/wiki/Datagram_Transport_Layer_Security
(6) https://upcommons.upc.edu/bitstream/handle/2117/98113/TJCF1de1.pdf
(7) https://www.francetvinfo.fr/monde/europe/un-journaliste-hackeur-s-introduit-dans-une-videoconference-confidentielle-de-l-ue_4190113.html
(8) https://w3c.github.io/webrtc-ice/
(9) https://www.monpetitforfait.com/vpn/aides/fuite-webrtc
(10) https://en.wikipedia.org/wiki/Traversal_Using_Relays_around_NAT
(11) https://www.rfc-editor.org/rfc/rfc7376.html#page-4
(12) https://www.zataz.com/fuite-de-donnees-pour-vpn-votre-ip-cachee-pas-cachee/
(13) https://link.springer.com/chapter/10.1007%2F978-3-030-01704-0_19
(14) https://www.mdpi.com/1999-5903/12/5/92/pdf
(15) https://vulners.com/hackerone/H1:843256
(16) https://www.journaldunet.fr/web-tech/guide-de-l-entreprise-digitale/1149771-slack-comment-l-utiliser-pour-gagner-en-efficacite240821/
(17) https://www.rtcsec.com/article/slack-webrtc-turn-compromise-and-bug-bounty/
(18) https://fr.wikipedia.org/wiki/Chiffrement_de_bout_en_bout
(19) https://www.frontlinedefenders.org/fr/resource-publication/guide-secure-group-chat-and-conferencing-tools
(20) https://www.al-enterprise.com/fr-fr/rainbow/telecharger-app
(21) https://www.ssi.gouv.fr/entreprise/certification_cspn/tixeoserver-version-11-5-2-0/
(22) https://www.webinarplease.com

Crédit image : Istock