Zoom accepte de payer 85 millions de dollars pour avoir menti sur le chiffrement de son application

Et envoyé des données à Facebook et Google à l'insu des utilisateurs

Le 3 août 2021 à 19:24, par Stéphane le calme | **30 commentaires**

105 PARTAGES

10 0

Zoom est l'un des grands bénéficiaires de cette pandémie : il a connu une hausse de son utilisation, en passant de 10 millions en décembre 2019 à 300 millions d'utilisateurs actifs par jour en avril 2020. Le revers de la médaille a été une attention particulière portée à l'application, notamment par les experts en sécurité et les régulateurs, dont la FTC. Ainsi, dès le mois de mars 2020, des bogues ont été relevés dans l'application et il a aussi été découvert que les réunions Zoom ne supportaient pas le chiffrement de bout en bout, ce qui donne la possibilité à l'entreprise d'espionner les réunions vidéo privées.

« Depuis au moins 2016, Zoom a induit les utilisateurs en erreur en prétendant qu'il offrait "un chiffrement de bout en bout à 256 bits" pour sécuriser les communications des utilisateurs, alors qu'en fait il offrait un niveau de sécurité inférieur », a déclaré en novembre 2020 la FTC dans l'annonce de sa plainte contre Zoom et de l'accord de principe. « Zoom a, en réalité, conservé les clés de chiffrement qui pouvaient lui permettre d'accéder au contenu des réunions de ses clients, et a sécurisé ses réunions Zoom, en partie, avec un niveau de cryptage inférieur à celui promis », a ajouté le régulateur.

Selon la plainte de la FTC, l'entreprise s'est jouée des utilisateurs de sa plateforme, pourtant importante pour leurs activités, alors qu'elle avait la possibilité et les moyens techniques pour mettre en place une sécurité théoriquement à l'épreuve des espions. En outre, la FTC estime que les affirmations trompeuses de Zoom ont donné aux utilisateurs un faux sentiment de sécurité, en particulier pour ceux qui ont utilisé la plateforme de l'entreprise pour discuter de sujets sensibles, tels que la santé et les informations financières, pour ne citer que ceux-là.

Par exemple, Zoom a affirmé offrir un chiffrement de bout en bout dans ses guides de conformité à la HIPAA (Health Insurance Portability and Accountability Act) de juin 2016 et juillet 2017, qui étaient destinés aux utilisateurs du service de vidéoconférence dans le secteur de la santé. Dans de nombreux articles de blogue, Zoom a spécifiquement fait valoir son niveau de chiffrement comme une raison pour les clients et les clients potentiels d'utiliser les services de vidéoconférence de Zoom. Cela dit, dans tous les cas, il s'agit de déclarations trompeuses.

La plainte souligne aussi que Zoom a affirmé qu'il offrait un chiffrement de bout en bout dans un livre blanc de janvier 2019, dans un article de blog d'avril 2017 et dans des réponses directes aux demandes de clients et de clients potentiels. Toujours selon la plainte de la FTC, Zoom a également induit en erreur certains utilisateurs qui voulaient stocker des réunions enregistrées sur le stockage en ligne de l'entreprise en prétendant à tort que ces réunions étaient chiffrées immédiatement après la fin de la réunion.

Cependant, au lieu de cela, certains enregistrements auraient été stockés de façon non chiffrée pendant 60 jours sur les serveurs de Zoom avant d'être transférés sur son stockage en ligne sécurisé. Pour régler ces allégations, Zoom a accepté l'obligation d'établir et de mettre en œuvre un programme de sécurité complet, l'interdiction de toute fausse déclaration sur la vie privée et la sécurité, et d'autres mesures détaillées et spécifiques pour protéger sa base d'utilisateurs.

En outre, le personnel de Zoom devra examiner toute mise à jour du logiciel pour détecter les failles de sécurité et s'assurer que les mises à jour n'entraveront pas les fonctions de sécurité de tiers. Par ailleurs, la résolution n'a pas de volet financier, mais le régulateur a déclaré que Zoom serait confrontée à des amendes pouvant aller jusqu'à 43 280 dollars pour chaque violation future de l'accord.

La plainte et le règlement de la FTC couvrent également le déploiement controversé par Zoom du serveur Web ZoomOpener qui a contourné les protocoles de sécurité d'Apple sur les ordinateurs Mac. « Le serveur Web ZoomOpener a permis à Zoom de se lancer automatiquement et de joindre un utilisateur à une réunion en contournant la protection du navigateur Safari d'Apple qui protégeait les utilisateurs contre un type de logiciel malveillant courant », a déclaré la FTC. En effet, Zoom a « secrètement installé » le logiciel dans le cadre d'une mise à jour de Zoom pour Mac en juillet 2018.

Zoom accepte de payer 85 millions de dollars pour mettre fin à un recours collectif

Zoom a accepté de payer 85 millions de dollars pour régler les allégations selon lesquelles il aurait menti sur le fait d'offrir un chiffrement de bout en bout et aurait communiqué les données des utilisateurs à Facebook et Google sans le consentement des utilisateurs. Le règlement entre Zoom et les déposants d'un recours collectif couvre également les problèmes de sécurité qui ont conduit à des *Zoombombings* endémiques.

Le règlement proposé donnerait généralement aux utilisateurs de Zoom 15 $ ou 25 $ chacun et a été déposé samedi devant le tribunal de district américain du district nord de Californie. Cela s'est produit neuf mois après que Zoom a accepté des améliorations de la sécurité et une « interdiction des fausses déclarations en matière de confidentialité et de sécurité » dans un règlement avec la Federal Trade Commission, mais le règlement de la FTC n'incluait pas de compensation pour les utilisateurs.

Le nouveau règlement de recours collectif s'applique aux utilisateurs de Zoom à l'échelle nationale des USA, qu'ils aient utilisé Zoom gratuitement ou payé pour un compte. Si le règlement est approuvé par le tribunal, « les membres du groupe qui ont payé pour un compte seront éligibles pour recevoir 15 % de l'argent qu'ils ont payé à Zoom pour leur abonnement de base aux réunions Zoom pendant cette période [du 30 mars 2016 au 30 juillet. 2021] ou 25 $, selon le montant le plus élevé », indique le règlement. « Les membres du groupe qui ne sont pas admissibles à soumettre une réclamation d'abonnement payé peuvent faire une réclamation de 15 $. Ces montants peuvent être ajustés, au prorata, à la hausse ou à la baisse, selon le volume de la réclamation, le montant des frais et dépenses, les paiements de service aux représentants de classe, les taxes et frais fiscaux, et les frais d'administration du règlement.

Les avocats du groupe obtiendraient des honoraires allant jusqu'à 25 pour cent des 85 millions de dollars et jusqu'à 200 000 $ pour le remboursement des dépenses. Environ une douzaine de plaignants nommés demandent l'approbation de paiements de 5 000 $ chacun. Une audience sur la requête des plaignants pour l'approbation préliminaire du règlement est prévue pour le 21 octobre 2021.

En plus des paiements, Zoom « a accepté plus d'une douzaine de changements majeurs à ses pratiques, conçus pour améliorer la sécurité des réunions, renforcer les divulgations de confidentialité et protéger les données des consommateurs », indique le règlement.

La pandémie augmentant son activité de visioconférence, Zoom a plus que quadruplé son chiffre d'affaires annuel, passant de 622,7 millions de dollars à 2,7 milliards de dollars au cours des 12 mois se terminant le 31 janvier 2021. Zoom a également déclaré un bénéfice net de 672 millions de dollars pour la période de 12 mois, contre 25,3 millions de dollars l'année dernière. Zoom est sur la bonne voie pour obtenir des résultats encore meilleurs cette année, avec un chiffre d'affaires du premier trimestre (février-avril) de 956,2 millions de dollars et un bénéfice net de 227,5 millions de dollars.

Zoom ne peut pas redéfinir ce qu'est le chiffrement de bout en bout

Une plainte de recours collectif modifiée déposée en mai 2021 indiquait que, malgré les fausses promesses de chiffrement de bout en bout (E2E) de Zoom, « les clés de chiffrement de chaque réunion sont générées par les serveurs de Zoom, et non par les appareils clients ».

Elle se poursuit ainsi :

« La connexion entre l'application Zoom exécutée sur l'ordinateur ou le téléphone d'un utilisateur et le serveur de Zoom est chiffrée de la même manière que la connexion entre un navigateur Web et un site Web est chiffrée. C'est ce qu'on appelle le chiffrement de transport, qui est différent du chiffrement de bout en bout, car le service Zoom lui-même peut accéder au contenu vidéo et audio non chiffré des réunions Zoom. Lors d'une réunion Zoom utilisant cette technologie de chiffrement, le contenu vidéo et audio restera privé de toute personne espionnant le Wi-Fi, mais ne restera pas privé de l'entreprise ou, vraisemblablement, de toute personne avec qui l'entreprise partage volontairement son accès, par contrainte de la loi (par exemple, à la demande des forces de l'ordre), ou involontairement (par exemple, un pirate informatique qui peut infiltrer les systèmes de l'entreprise). Avec un véritable chiffrement E2E, les clés de chiffrement sont générées par les appareils des utilisateurs (clients) et seuls les participants à la réunion ont la possibilité de les déchiffrer ».

Le site Web de Zoom a affirmé que son service permet à un hôte « sécuriser une réunion avec un chiffrement de bout en bout » et que « la solution et l'architecture de sécurité de Zoom fournissent un chiffrement de bout en bout et des contrôles d'accès aux réunions afin que les données en transit ne puissent pas être interceptées », selon la plainte. Mais Zoom n'a pas droit à sa propre définition du chiffrement de bout en bout, a déclaré le recours collectif. « La définition du chiffrement de bout en bout n'est pas à interpréter dans l'industrie », a déclaré la plainte. « Les fausses déclarations de Zoom contrastent fortement avec d'autres services de visioconférence, tels que FaceTime d'Apple, qui ont entrepris la tâche la plus difficile de mettre en œuvre un véritable chiffrement E2E pour un appel à plusieurs parties ».

Partage des données utilisateurs et *Zoombombings*

Les utilisateurs de Zoom se sont appuyés sur les promesses de l'entreprise selon lesquelles « Zoom ne vend pas les données des utilisateurs » et que « Zoom prend la confidentialité au sérieux et protège adéquatement les informations personnelles des utilisateurs », a déclaré la plainte. Les membres du groupe ne comprenaient pas que « Zoom recueillerait et partagerait [leurs] renseignements personnels avec des tiers, y compris Facebook et Google » et « autoriserait des tiers, comme Facebook et Google, à accéder à [leurs] renseignements personnels et à les combiner avec du contenu et des informations provenant d'autres sources pour créer un identifiant ou un profil unique de [chaque utilisateur] à des fins publicitaires et influençant le comportement », peut-on lire par la suite.

Étant donné que Zoom a implémenté le SDK Facebook, les données de l'utilisateur ont été envoyées par Zoom à Facebook « que l'utilisateur ait créé un compte Zoom ou Facebook, et, pire encore, avant même que l'utilisateur n'ait accédé à la rubrique termes et conditions de Zoom ou toute rubrique concernant la confidentialité », a déclaré la plainte. Bien que Zoom aurait depuis « supprimé le SDK Facebook, Zoom continue de partager des données utilisateur tout aussi précieuses avec Google via le SDK Firebase Analytics de Google, également intégré à l'application Zoom. Les plaignants n'ont jamais accordé l'autorisation à des tiers d'extraire et d'utiliser ces données – en effet, ils n'étaient même pas au courant de la transmission des données ». Outre Facebook et Google, Zoom « envoie des données personnelles sur leurs utilisateurs à hotjar, Zendesk, AdRoll, Bing et autres ».

La plainte a également déclaré que Zoom a blâmé les utilisateurs pour une éruption de Zoombombings même si le problème a été activé par les lacunes de sécurité de Zoom. Zoom pourrait avoir des interruptions de réunion limitées par des participants non autorisés avec « des solutions techniques relativement simples... par exemple, permettant aux hôtes d'annuler plus facilement une réunion et/ou d'éjecter un Zoombomber en appuyant sur un seul bouton, des paramètres de contrôle de partage d'écran par défaut, ou mettre en œuvre des protocoles plus stricts de sécurité des réunions (admission des participants) tels que la vérification de

appuyant sur un seul bouton, des paramètres de contrôle de partage d'écran par défaut, ou mettre en œuvre des protocoles plus stricts de sécurité des réunions (admission des participants) tels que la vérification de l'identité ou des codes d'accès uniques pour les réunions », a déclaré la plainte.

« Dès le 20 mars 2020, Zoom a admis que son produit avait un problème avec Zoombombing. Plutôt que de modifier les protocoles de sécurité et les fonctionnalités par défaut, Zoom a tourné le dos à ses utilisateurs, affirmant qu'ils étaient à blâmer pour leur incapacité à utiliser correctement le programme », a déclaré la plainte.

Exigences du règlement

Pour régler cette affaire, la plainte « exige que Zoom ne réintègre pas le SDK Facebook pour iOS dans les réunions Zoom pendant un an » et demande à Facebook de « supprimer toutes les données d'utilisateur américain obtenues à partir du SDK ». Les changements de sécurité et de transparence que Zoom a acceptés incluent les éléments suivants :

- Développer et maintenir, pendant au moins trois ans, des protocoles et des procédures documentés pour l'admission d'applications tierces à diffuser aux utilisateurs via le « Marketplace » de Zoom.
- Développer et maintenir un système de ticket d'assistance aux utilisateurs pour le suivi interne et la communication avec les utilisateurs au sujet des rapports d'interruption de réunion.
- Développer et maintenir un processus documenté de communication avec les forces de l'ordre au sujet des perturbations de réunion impliquant un contenu illégal, y compris du personnel dédié pour signaler les perturbations de réunions en série aux forces de l'ordre.
- Développer et maintenir des fonctionnalités de sécurité telles que des salles d'attente pour les participants, le bouton de suspension des activités de réunion et le blocage des utilisateurs de pays spécifiques pendant au moins trois ans.

Zoom devra « mieux informer les utilisateurs sur les fonctionnalités de sécurité disponibles pour protéger la sécurité et la confidentialité des réunions, via un espace dédié sur le site Web de Zoom et des notifications de type bannière ». Le site Web de Zoom devra également inclure « des informations centralisées et des liens pour les parents dont les enfants utilisent des comptes K-12 fournis par l'école ».

Après l'annonce du règlement, Zoom a donné aux médias une déclaration qui n'admettait aucun acte répréhensible : « La confidentialité et la sécurité de nos utilisateurs sont des priorités absolues pour Zoom, et nous prenons au sérieux la confiance que nos utilisateurs nous accordent », a déclaré Zoom. « Nous sommes fiers des progrès que nous avons réalisés sur notre plateforme et sommes impatients de continuer à innover en mettant la confidentialité et la sécurité au premier plan ».

Source : plaintes (1, 2)

Et vous ?