Piratage Google Home : des conversations privées sur écoute

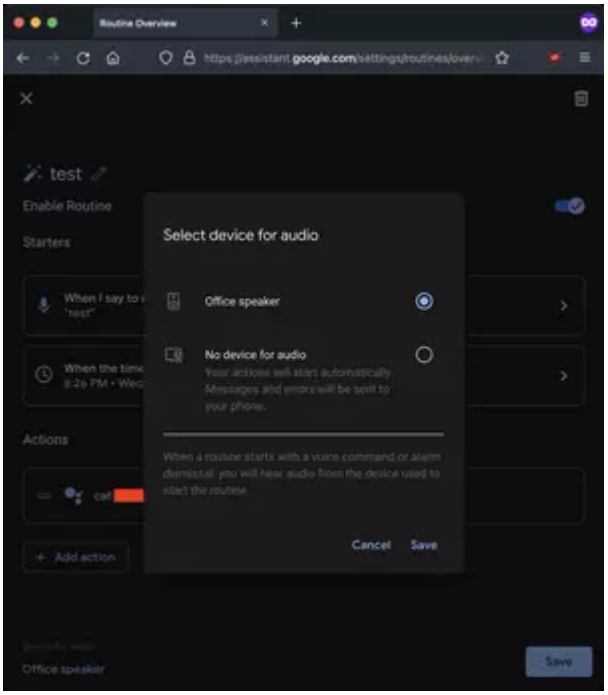
Maurine Briantais 30/12/22 14:54

On ne se méfie jamais assez des appareils connectés ! Un chercheur a découvert une faille de sécurité permettant à des pirates d'écouter les conversations autour des enceintes Google Home Mini pour espionner leurs utilisateurs.

Les enceintes connectées peuvent-elles servir à de l'espionnage ? C'est la question que s'est posée Matt Kunze, un chercheur en sécurité informatique, qui s'est livré à une expérience très instructive. Ainsi, en janvier 2021, il a découvert une étonnante faille de sécurité dans les enceintes connectées Google Home Mini – depuis rebaptisé Nest Mini –, comme le rapporte Bleeping Computer. Il a immédiatement prévenu la firme de Mountain View, qui l'a récompensé d'une somme de 107 500 dollars pour sa trouvaille et qui a corrigé le problème en avril 2021 via une mise à jour automatique. Ce n'est qu'en cette fin d'année 2022 que le chercheur a publié des détails techniques ainsi qu'un scénario d'attaque pour montrer comment la faille pouvait être exploitée. Ainsi, des pirates pouvaient prendre le contrôle de l'enceinte intelligente à distance et espionner les conversations autour d'elle en accédant au microphone. Heureusement, la manipulation était loin d'être simple et elle se limitait à un modèle d'appareil en particulier, ce qui a réduit le risque de piratage massif. mais elle pointe du doigt une potentielle utilisation malveillante de ces enceintes connectées, pourtant si pratiques, pour récolter des données privées…

Google Home Mini : un micro sous contrôle

Le chercheur a découvert que, sur une Google Home Mini, les nouveaux comptes utilisateurs ajoutés à partir de l'application Google Home étaient capables d'envoyer des commandes à distance depuis l'interface de programmation de l'application (API) dans le cloud. De quoi intéresser les personnes mal intentionnées ! Pour s'ajouter comme utilisateur sans avoir le mot de passe Wi-Fi de la victime, il suffisait de connaitre le nom de l'appareil, le certificat et l'identifiant cloud de l'API locale pour envoyer une demande de lien au serveur Google en reproduisant la demande de liaison dans un script Python. À partir de là, c'était la porte ouverte à toute sorte d'abus. Ces failles ont pu être exploitées depuis 2018, date à laquelle les routines planifiées ont été lancées.



Le routage malveillant qui capture l'audio du micro © Bleeping Computer

En effet, l'enceinte permet d'effectuer toutes sortes de commandes dans la maison, comme déverrouiller à distance des serrures connectées, réaliser des achats en ligne, fermer ou ouvrir les volets – très pratique pour un cambriolage –, renommer l'enceinte, forcer son redémarrage, lui faire oublier les réseaux Wi-Fi stockés, forcer de nouveaux couplages Bluetooth ou Wi-Fi et lire des médias dessus. Mais, surtout, le pirate peut abuser de la commande "appeler [numéro de téléphone]" en l'ajoutant à une routine. Elle permet d'activer le micro en même temps que le lancement d'un appel vers le numéro du hacker, qui a ainsi tout le loisir d'écouter les conversations qui se déroulent autour de l'appareil compromis. Le seul moyen pour la victime de savoir que son appareil l'espionne est l'affichage en bleu de ses LED, qui clignotent lorsque le microphone est activé.

Heureusement, Google a depuis ajouté une protection pour empêcher le déclenchement de la commande à distance par des routines. C'est pourquoi, on ne le rappellera jamais assez, il est primordial de vérifier que les mises à jour de sécurité de ses appareils – et pas que le Google Home Mini – soient régulièrement faites. À noter que certains possèdent des fonctions pour bloquer physiquement l'accès à un microphone ou à la caméra.