Empêcher les fuites d'adresses IP liées à WebRTC

Guillaume Nibert*†[1,2], Sébastien Tixeuil[1,3], Baptiste PolvÉ[2], Nana J. Bakalafoua M'boussi[2], and Xuan Son Nguyen[2]

[1]LIP6 – Sorbonne Universite, Centre National de la Recherche Scientifique, Centre National de la Recherche Scientifique : UMR7606 – France

[2]Snowpack – Snowpack – France

[3]Institut Universitaire de France – Ministère de l'Education nationale, de l'Enseignement supérieur et
de la Recherche, Ministère de lÉducation nationale, de l'Enseignement supérieur et de la Recherche,
Ministère de lÉducation nationale, de l'Enseignement supérieur et de la Recherche, Ministère de
lÉducation nationale, de l'Enseignement supérieur et de la Recherche, Ministère de lÉducation
nationale, de l'Enseignement supérieur et de la Recherche, Ministère de lÉducation nationale, de
l'Enseignement supérieur et de la Recherche, Ministère de lÉducation nationale, de l'Enseignement
supérieur et de la Recherche, Ministère de lÉducation nationale, de l'Enseignement supérieur et de la
Recherche, Ministère de lÉducation nationale, de l'Enseignement supérieur et de la Recherche, Ministère
de lÉducation nationale, de l'Enseignement supérieur et de la Recherche, Ministère de lÉducation
nationale, de l'Enseignement supérieur et de la Recherche, Ministère de lÉducation nationale, de
l'Enseignement supérieur et de la Recherche, Ministère de lÉducation nationale, de l'Enseignement
supérieur et de la Recherche, Ministère de lÉducation nationale, de l'Enseignement supérieur et de la
Recherche, Ministère de lÉducation nationale, de l'Enseignement supérieur et de la Recherche,
Ministère de lÉducation nationale, de l'Enseignement supérieur et de la Recherche, Ministère de
lÉducation nationale, de l'Enseignement supérieur et de la Recherche, Ministère de lÉducation
nationale, de l'Enseignement supérieur et de la Recherche, Ministère de lÉducation nationale, de
l'Enseignement supérieur et de la Recherche, Ministère de lÉducation nationale, de l'Enseignement
supérieur et de la Recherche, Ministère de lÉducation nationale, de l'Enseignement supérieur et de la
Recherche, Ministère de lÉducation nationale, de l'Enseignement supérieur et de la Recherche,
Ministère de lÉducation nationale, de l'Enseignement supérieur et de la Recherche, Ministère de
lÉducation nationale, de l'Enseignement supérieur et de la Recherche, Ministère de lÉducation
nationale, de l'Enseignement supérieur et de la Recherche, Ministère de lÉducation nationale, de
l'Enseignement supérieur et de la Recherche, Ministère de lÉducation nationale, de l'Enseignement
supérieur et de la Recherche, Ministère de lÉducation nationale, de l'Enseignement supérieur et de la
Recherche, Ministère de lÉducation nationale, de l'Enseignement supérieur et de la Recherche,
Ministère de lÉducation nationale, de l'Enseignement supérieur et de la Recherche, Ministère de
lÉducation nationale, de l'Enseignement supérieur et de la Recherche, Ministère de lÉducation
nationale, de l'Enseignement supérieur et de la Recherche, Ministère de lÉducation nationale, de
l'Enseignement supérieur et de la Recherche, Ministère de lÉducation nationale, de l'Enseignement
supérieur et de la Recherche, Ministère de lÉducation nationale, de l'Enseignement supérieur et de la
Recherche, Ministère de l'Education nationale, de l'Enseignement supérieur et de la Recherche – France

Résumé

*Intervenant

†Auteur correspondant: guillaume.nibert@snowpack.eu

L'API WebRTC permet la communication en temps réel de flux médias textes, vidéos et audios par l'intermédiaire d'un navigateur web sans nécessiter d'extensions tierces. Cependant, elle n'a pas été conçue en tenant compte de la protection de la vie privée. C'est pourquoi, nous menons une expérience pour analyser les fuites de données privées associées à WebRTC. Nos résultats montrent que, malgré les récentes mises à jour de la spécification WebRTC et de ses implémentations, des adresses IP publiques sensibles peuvent encore être divulguées pendant les communications audio/vidéo, en particulier dans les grands réseaux d'entreprise dépourvus de NAT, et ce même caché derrière un VPN. Pour remédier aux fuites observées, nous avons développé une solution simple, facilement maintenable et multiplateforme qui confine le navigateur web Mozilla Firefox dans un conteneur Docker. Nous prenons également en compte la possibilité qu'un adversaire malveillant puisse compromettre le navigateur. Nos tests démontrent que notre solution conteneurisée est efficace dans toutes les situations sans restreindre les applications.