ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité
des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

NOTE DE SECURITE

Titre	"Polyfill.io" Supply Chain Attack
Numéro de Référence	48371207/24
Date de Publication	12 Juillet 2024
Risque	Critique
Impact	Critique

Une vulnérabilité a été identifiée concernant l'utilisation de Polyfill.io, un service populaire de polyfills JavaScript largement implémenté dans des applications Webs. Une compagne d'attaque par supply chain est détectée qui permet à des acteurs malveillants d'injecter du code compromis via ce service, affectant ainsi les applications web qui l'utilisent. Les attaquants ont pu modifier les fichiers polyfills hébergés sur Polyfill.io, entraînant l'exécution de code malveillant dans les navigateurs des utilisateurs finaux.

Cette attaque peut mener à des vols de données, des redirections vers des sites malveillants, ou même à la prise de contrôle de l'environnement d'exécution des utilisateurs.

Recommandations :

- Mise à jour immédiate : Vérifiez les versions des polyfills utilisés dans vos projets et supprimer immédiatement celui de « Polyfill.io ».
- Audit de sécurité : Réalisez un audit de sécurité de votre code et de vos dépendances pour identifier d'éventuelles failles.
- Utilisation de CDNs de confiance : Évaluez l'utilisation de Content Delivery Networks (CDNs) pour charger des polyfills, en choisissant des sources réputées.
- Surveillance : Mettez en place des mécanismes de surveillance pour détecter des comportements suspects dans vos applications.

Référence :

- https://thehackernews.com/2024/07/polyfillio-attack-impacts-over-380000.html
- https://censys.com/july-2-polyfill-io-supply-chain-attack-digging-into-the-web-of-compromised-domains/

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات, مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma