Digital Services
Case Study

Un fournisseur de services numériques renforce la sécurité de ses applications grâce à JFrog Curation

Blocage immédiat des packages malveillants

Prévention des futures attaques contre la chaîne d'approvisionnement

Passage d'une sécurité réactive à une sécurité proactive

+ de 4 mrd.	6K	+ de 20 mio.
Chiffre d'affaires	Employés	Utilisateurs

Ce fournisseur de services numériques de premier plan a été en mesure de protéger sa chaîne d'approvisionnement logicielle lors de la récente série d'attaques npm grâce à la plateforme JFrog et au déploiement rapide de JFrog Curation.

LE DÉFI

Répondre à une attaque massive ciblant l'écosystème npm

De nombreuses entreprises de services numériques de premier plan s'appuient sur des packages open source pour accélérer la livraison et garantir la qualité de leurs produits et services. Pour ce faire, ils s'appuient sur les principaux dépôts de logiciels open source (OSS), tels que npm, PyPI, GitHub et d'autres. Malheureusement, elles figurent parmi les organisations les plus impactées par la récente attaque massive contre npm.

Dans un cas similaire, plus de 80 versions distinctes de packages ont été identifiées comme malveillantes. Bien que l'équipe ait effectué des scans approfondis des vulnérabilités et des non-conformités de licence, elle a vite compris qu'un code malveillant pouvait déjà s'être introduit dans son environnement de développement sans avoir été repéré.

Dans un premier temps, l'équipe DevSecOps a dû identifier et retirer de ses systèmes l'ensemble des packages susceptibles d'avoir été compromis. Cette approche réactive a mobilisé un temps critique lors d'un incident à haut risque et peut, en l'absence de traitement rapide, provoquer une perte importante de confiance des clients, voire des répercussions financières.

À la suite de cet incident et en suivant les dernières tendances du secteur, les équipes DevOps et de sécurité ont pris la décision stratégique d'adopter une approche shift-left, avec pour objectif d'arrêter les packages malveillants avant même qu'ils ne puissent pénétrer dans leur environnement de développement.

> *Ce qui rend ce cas si intéressant, c'est la façon dont la réaction rapide à un incident critique s'est transformée en une transformation stratégique durable de la sécurité.*

LA SOLUTION

Mise en œuvre rapide de JFrog Curation dans la production

Bien que l'équipe ait déjà une certaine expérience de JFrog Curation, elle était désormais prête à explorer en profondeur ses fonctionnalités et à évaluer les modalités de mise en œuvre dans les plus brefs délais. Déjà utilisateurs de JFrog Xray, les membres de l'équipe ont pu déployer rapidement le puissant moteur de gouvernance et d'application automatique des politiques de Curation, placé en amont de la chaîne d'approvisionnement logicielle et intégré à leur processus de production.

Selon l'un des membres de l'équipe, après le déploiement immédiat de Curation, la priorité suivante était claire :

> *« Passer d'une sécurité réactive à une sécurité proactive dès que possible. »*

Accompagnés par l'équipe JFrog et les experts de JFrog Professional Services, ils ont lancé la mise en place de politiques Curation destinées à :

- Bloquer les packages malveillants connus dans les dépôts publics avant que les développeurs ne puissent les intégrer dans l'environnement de développement ;
- Appliquer la politique de téléchargement de packages à partir de sources fiables uniquement et éliminer le risque de dépendances typosquattées ou compromises ;
- Contrôler en permanence les packages open source et leurs dépendances afin de prévenir les futures attaques de la chaîne d'approvisionnement.

À peine quelques jours après la mise en service, l'impact était déjà visible : des composants OSS autrefois acceptés et intégrés sans difficulté au code étaient désormais soumis à un contrôle automatique et stoppés en périphérie.

LES RÉSULTATS

Une protection proactive à un moment décisif

En activant JFrog Curation, l'équipe DevSecOps a été en mesure de :

- Neutraliser immédiatement les packages npm malveillants d'entrer dans leur environnement ;
- Commencer la mise en œuvre de la sécurité shift-left en stoppant les packages à risque avant qu'ils n'atteignent les développeurs ou les systèmes de production ;
- Simplifier la mise en conformité et l'application des politiques à travers les dépendances open source ;
- Rétablir la confiance dans l'utilisation des logiciels open source lors de l'une des plus graves attaques de npm à ce jour.

> *Ce qui a commencé comme une réponse à un incident critique s'est transformé en une transformation de la sécurité durable et significativement bénéfique !*

En intégrant JFrog Curation à Xray, l'organisation bénéficie désormais d'une posture de sécurité de la chaîne d'approvisionnement logicielle améliorée qui permet non seulement d'identifier les vulnérabilités, mais aussi de les empêcher d'entrer dans leur écosystème.

JFrog a aidé ce client à passer d'une réaction aux menaces à une prévention proactive, protégeant ainsi les développeurs, l'infrastructure et les clients. Planifiez une démonstration, faites une visite en ligne ou commencez un essai gratuit pour voir comment vous pouvez commencer à sécuriser votre chaîne d'approvisionnement en logiciels de manière proactive.

v1.0240129

www.jfrog.com

www.twitter.com/jfrog

www.facebook.com/artifrog/

www.linkedin.com/company/jfrog-ltd