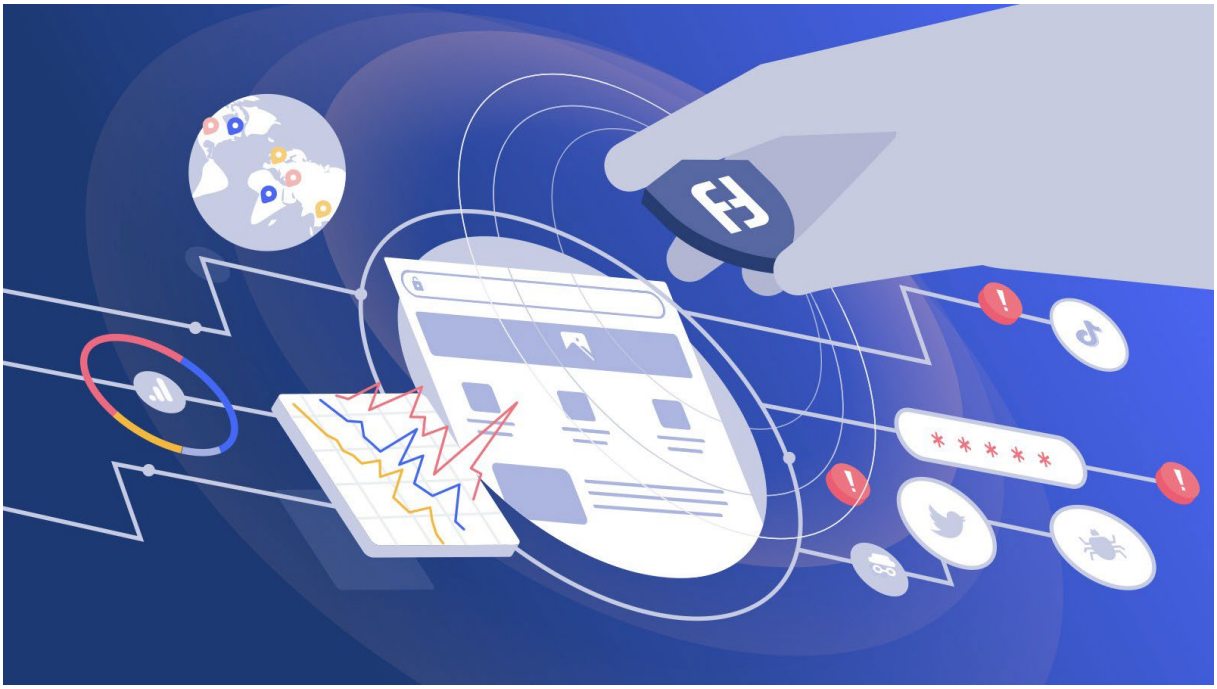
https://www.reflectiz.com/blog/do-you-really-trust-your-web-app-supply-chain/

Faites-vous vraiment confiance à la chaîne d'approvisionnement de vos applications web ?



17 octobre 2023 Temps de lecture : 4 min

Eh bien, vous ne devriez pas. Elle cache peut-être déjà des vulnérabilités.

Publié à l'origine sur The Hacker News ici.

C'est la nature modulaire des applications web modernes qui les a rendues si efficaces. Elles peuvent faire appel à des dizaines de composants Web tiers, de frameworks JS et d'outils open source pour fournir toutes les différentes fonctionnalités qui satisfont leurs clients, mais cette chaîne de dépendances est aussi ce qui les rend si vulnérables.

Bon nombre de ces composants de la chaîne d'approvisionnement des applications Web sont contrôlés par un tiers, l'entreprise qui les a créés. Cela signifie que, quelle que soit la rigueur de votre propre analyse statique du code, de vos révisions de code, de vos tests d'intrusion et d'autres processus SSDLC (cycle de vie du développement logiciel sécurisé), la majeure partie de la sécurité

de votre chaîne d'approvisionnement est entre les mains de la personne qui a construit ses composants tiers.

Avec leur énorme potentiel de points faibles et leur utilisation généralisée dans les secteurs lucratifs du commerce électronique, de la finance et de la santé, les chaînes d'approvisionnement d'applications Web constituent une cible juteuse pour les cyberattaquants. Ils peuvent cibler n'importe lequel des dizaines de composants auxquels leurs utilisateurs font confiance pour infiltrer leurs organisations et compromettre leurs produits. Les logiciels, les bibliothèques tierces et même les appareils IoT sont régulièrement attaqués parce qu'ils offrent un moyen d'obtenir un accès privilégié aux systèmes tout en restant indétectables. À partir de là, les attaquants peuvent émettre des attaques Magecart et d'écrémage Web, des rançongiciels, commettre de l'espionnage commercial et politique, utiliser leurs systèmes pour le minage de cryptomonnaies, ou même simplement les vandaliser.

L'attaque SolarWinds

En décembre 2020, une attaque de la chaîne d'approvisionnement a été découverte qui en éclipse beaucoup d'autres en termes d'échelle et de sophistication. Elle ciblait une plate-forme de surveillance des réseaux et des applications nommée Orion qui est fabriquée par une société appelée SolarWinds. Les attaquants avaient secrètement infiltré son infrastructure et utilisé leurs privilèges d'accès pour créer et distribuer des mises à jour piégées aux 18 000 utilisateurs d'Orion.

Lorsque ces clients ont installé les mises à jour compromises de SolarWinds, les attaquants ont eu accès à leurs systèmes et ont eu carte blanche pendant des semaines. Des agences gouvernementales américaines ont été compromises, ce qui a déclenché des enquêtes qui ont pointé du doigt une opération de l'État russe.

Cette attaque dévastatrice de la chaîne d'approvisionnement peut également se produire dans les environnements Web, et elle souligne la nécessité d'une solution de sécurité Web complète et proactive qui surveillera en permanence vos actifs Web.

Les outils de sécurité standard sont déjoués

Les processus de sécurité standard n'ont pas été d'une grande aide avec SolarWinds et ils ne peuvent pas surveiller l'ensemble de votre chaîne d'approvisionnement. Il existe de nombreux domaines de risque potentiels qu'ils manqueront tout simplement, tels que :

- **Les règles de confidentialité et de sécurité** : Si l'un de vos fournisseurs tiers publie une nouvelle version qui n'est pas conforme aux réglementations en matière de sécurité et de confidentialité, les outils de sécurité traditionnels ne prendront pas en charge ce changement.
- **Les traqueurs et pixels.** Dans le même ordre d'idées, si votre gestionnaire de balises est mal configuré d'une manière ou d'une autre, il peut collecter par inadvertance des informations personnellement identifiables, vous exposant à d'éventuelles (énormes !) pénalités et poursuites judiciaires.
- **Les serveurs externes :** Si le serveur externe qui héberge votre framework JS est piraté, vous ne serez pas alerté.
- **Les vulnérabilités de pré-production :** Si une nouvelle vulnérabilité apparaît une fois que vous êtes passé en production, vous ne pourrez peut-être pas l'atténuer.

Dans ces situations et dans bien d'autres, les outils de sécurité standards ne suffiront pas.

La vulnérabilité Log4j

Une autre de ces situations s'est produite lorsqu'une vulnérabilité zero-day a été découverte dans le Log4j Utilitaire de journalisation basé sur Java. Des millions d'ordinateurs appartenant à des entreprises, des organisations et des particuliers dans le monde entier utilisent Log4j dans leurs services en ligne. Un correctif a été publié trois jours après la découverte de la vulnérabilité en 2021, mais selon les mots de Sean Gallagher, chercheur senior Sophos sur les menaces : « Honnêtement, la plus grande menace ici est que les gens ont déjà obtenu l'accès et restent assis dessus, et même si vous résolvez le problème, quelqu'un est déjà dans le réseau... Il restera aussi longtemps qu'Internet. »

Cette vulnérabilité permet aux pirates de prendre le contrôle d'appareils susceptibles d'être infectés par l'exploit via Java. Encore une fois, ils peuvent

ensuite utiliser ces appareils pour des activités illégales telles que le minage de crypto-monnaie, la création de botnets, l'envoi de spams, l'établissement de portes dérobées, Magecart, et le lancement d'attaques de ransomware.

Après sa divulgation, Check Point a signalé des millions d'attaques lancées par des pirates informatiques, et certains chercheurs ont observé un taux de plus de 100 attaques par minute et des tentatives d'attaques sur plus de 40 % des réseaux d'entreprise dans le monde.

Étant donné que votre chaîne d'approvisionnement d'applications Web pourrait déjà avoir été compromise par la vulnérabilité Log4J, le besoin d'une solution de surveillance continue proactive devient encore plus urgent.

L'une de ces solutions est une société de sécurité Web appelée Reflectiz. Sa plate-forme a détecté la vulnérabilité Log4J dans le domaine Bing de Microsoft à un stade précoce, qu'elle a rapidement corrigée. Ensuite, Reflectiz a analysé de manière proactive des milliers de sites Web et de services pour identifier d'autres vulnérabilités de Log4J. Une vulnérabilité importante a été découverte dans le composant de suivi de conversion de Microsoft - Universal Event Tracking (UET) , affectant des millions d'utilisateurs sur diverses plates-formes. Reflectiz a informé et collaboré avec ses clients et prospects pour atténuer les risques, en adhérant à des procédures de divulgation responsables en informant Microsoft et en partageant ses conclusions. Ils soulignent la nature continue de l'événement Log4J et plaide pour que les organisations sécurisent leurs sites Web en s'attaquant aux vulnérabilités de tiers.

Sécurisation de la chaîne d'approvisionnement de vos applications web

L'interaction de vos composants Web internes et tiers dans votre Chaîne d'approvisionnement des applications Web crée un environnement dynamique et en constante évolution. Un environnement en constante évolution nécessite une solution de surveillance continue qui vous alerte des comportements suspects dans chaque élément de votre chaîne d'approvisionnement d'applications Web.

Grâce à une surveillance continue rigoureuse, les équipes de sécurité peuvent :

- **identifier** toutes les ressources Web existantes et **détecter** les vulnérabilités dans la chaîne d'approvisionnement Web et les composants open source
- **Monitorer** les configurations d'applications web et les paramètres de code tiers
- Avoir une **visibilité totale sur les risques** des vulnérabilités et des problèmes de conformité
- **Suivre les** accès des composants web aux données sensibles
- **Valider** les comportements de tiers