Un téléchargement de Log4j sur trois concerne des versions vulnérables

Selon la société Sonatype, les entreprises et les développeurs continuent de télécharger des versions de Log4j antérieures à celle corrigeant la faille Log4Shell et ses déclinaisons. Pour expliquer cet état de fait, les experts avancent plusieurs explications.

Voir l'article complet sur
https://www.lemondeinformatique.fr/actualites/lire-des-versions-de-log4j-vulnerables-sont-toujours-telechargees-86107.html

Comment rester vigilant et les actions à mener en tant que développeur ?

Il est important de s'assurer que les bibliothèques et les frameworks utilisés dans une application sont à jour et sécurisés. Les versions vulnérables de logiciels comme Log4j peuvent être exploitées par des pirates informatiques pour accéder à des données sensibles ou prendre le contrôle de l'application.

Il est recommandé de toujours utiliser la version la plus récente et la plus sécurisée de Log4j et de tous les autres logiciels utilisés dans votre application. Vous pouvez vérifier les versions disponibles de Log4j sur le site web du projet. Si vous utilisez une version vulnérable, il est recommandé de mettre à jour vers la version la plus récente dès que possible.

Il est également recommandé de configurer les alertes de sécurité et de suivre les annonces de sécurité pour être informé des vulnérabilités connues et des mises à jour de sécurité disponibles pour Log4j et d'autres logiciels utilisés dans votre application.

Il est possible que les versions vulnérables d'un logiciel soient toujours disponibles sur le dépôt officiel, mais elles ne sont généralement plus mises à jour et ne bénéficient plus de support. Les versions vulnérables peuvent être laissées en ligne pour des raisons de compatibilité avec des versions antérieures de l'application, mais il est recommandé de ne pas utiliser ces versions car elles peuvent être exploitées par des pirates informatiques.

Il existe plusieurs façons de se tenir au courant des alertes de sécurité et des mises à jour de sécurité

disponibles pour les logiciels que vous utilisez:

1. Suivre les annonces de sécurité du développeur ou du fournisseur du logiciel. De nombreux développeurs et fournisseurs de logiciels publient des annonces de sécurité sur leur site web ou sur leurs pages de réseaux sociaux, ou envoient des notifications par e-mail aux utilisateurs enregistrés.

2. S'inscrire aux alertes de sécurité de l'industrie. Il existe plusieurs organisations et sites web qui publient des alertes de sécurité pour les logiciels et les technologies populaires. Vous pouvez vous inscrire à leur liste de diffusion ou suivre leur compte sur les réseaux sociaux pour recevoir des notifications lorsqu'une alerte de sécurité est publiée.

- US-CERT: https://www.us-cert.gov/
- CERT Coordination Center: https://www.cert.org/
- SANS Institute: https://www.sans.org/
- National Vulnerability Database: https://nvd.nist.gov/
- SecurityFocus: https://www.securityfocus.com/
- The Open Web Application Security Project: https://www.owasp.org/

3. Utiliser des outils de suivi de sécurité. Il existe plusieurs outils qui vous permettent de configurer des alertes pour être informé des vulnérabilités connues et des mises à jour de sécurité disponibles pour les logiciels que vous utilisez. Ils peuvent être configurés pour envoyer des notifications par e-mail ou via les réseaux sociaux, ou pour afficher des notifications dans l'interface de l'outil. Certains outils de suivi de sécurité vous permettent également de scanner votre réseau pour détecter les vulnérabilités et de mettre en place des mesures de protection.

Pour les logiciels open source on peut citer :

- OpenVAS: https://www.openvas.org/
- Nessus: https://www.tenable.com/products/nessus
- Nexpose Community Edition: https://www.rapid7.com/products/nexpose/community-edition/
- OSSEC: https://ossec.github.io/
- Lynis: https://cisofy.com/lynis/

Pour les logiciels propriétaires :

- GFI LanGuard: https://www.gfi.com/products-and-solutions/network-security-vulnerability-management/languard
- Rapid7 Nexpose: https://www.rapid7.com/products/nexpose/
- Tenable Nessus: https://www.tenable.com/products/nessus
- Qualys Vulnerability Management: https://www.qualys.com/vulnerability-management/
- McAfee Vulnerability Manager: https://www.mcafee.com/enterprise/en-us/products/vulnerability-manager.html

Il est important de rester vigilant et de se tenir au courant des alertes de sécurité pour protéger votre application et vos données contre les vulnérabilités connues.

— *Cédric ABONNEL (cedricabonnel) - Publication initiale le Mardi 10 Janvier 2023*

Crédit image : *Midjourney*

From:
https://www.abonnel.fr/ - **notes informatique & technologie**

Permanent link:
https://www.abonnel.fr/journal_geek/2023/20230110-un-telechargement-de-log4j-sur-trois-concerne-des-versions-vulnerables

Last update: **2023/01/10 02:21**