A propos des logiciels libre (licence GNU).

QUESTION : De nombreuses applications sont gratuites en téléchargement. Ces applications sont en OPEN SOURCE, c'est à dire que le code est ouvert, disponible, donc éventuellement modifiables... A ce titre (*accès au code*) les applications libres sous Windows sont-elles plus vulnérables que les applications libres de Linux ?. En effet, les téléchargements des applications Linux se réalisent depuis des serveurs spécifiques Linux, alors qu'on trouve les applications libres Windoxs un peu partout, ce qui laisse un doute quant à l'inviolabilité du code source...

Que peux tu me préciser à ce sujet ?

RÉPONSE : Votre question touche à un point fondamental de la sécurité des logiciels libres. Vous avez raison de vous interroger : un code source ouvert est-il plus vulnérable simplement parce qu'il est accessible ?

La réponse courte est non, la vulnérabilité ne vient pas de l'ouverture du code en soi, mais bien de la manière dont on se procure et dont on installe ce code. C'est là que la différence entre l'écosystème Linux et l'écosystème Windows est la plus marquante.

🔍 Le vrai danger : la provenance du logiciel

Le cœur du problème que vous soulevez n'est pas la licence GNU ou l'open source, mais la **chaîne d'approvisionnement** du logiciel, c'est-à-dire le chemin qu'il parcourt du développeur à votre ordinateur.

Le modèle Linux : des dépôts officiels comme rempart

Sous Linux, vous avez raison, les applications s'installent presque exclusivement depuis des **dépôts officiels** (comme avec `apt` ou `dnf`). Ces dépôts sont la force de ce système.

- **Centralisation et confiance** : Ce sont des serveurs maintenus par la distribution (ex: Debian, Ubuntu). Ils contiennent des versions validées de logiciels .
- **Signature cryptographique** : Chaque paquet est signé. Votre gestionnaire de paquets vérifie ces signatures, vous garantissant que le logiciel que vous installez est authentique et n'a pas été altéré .

- **Mises à jour centralisées** : Une seule commande met à jour l'ensemble du système et des applications, ce qui permet de corriger très rapidement les failles de sécurité découvertes .

Ce système est conçu pour **minimiser les risques de téléchargement d'un logiciel malveillant**.

Le modèle Windows : l'océan du téléchargement

Sous Windows, la situation est très différente. Comme vous le constatez, les applications libres se téléchargent depuis une multitude de sites.

- **Le piège des faux sites** : Cette ouverture est exploitée par des cybercriminels qui créent des copies quasi parfaites de sites de projets open source légitimes .
- **Des techniques de plus en plus sophistiquées** : Certains de ces faux sites utilisent des systèmes pour ne rediriger que certains visiteurs (selon leur pays, par exemple) vers des versions infectées du logiciel . D'autres affichent un lien vers le site officiel, mais le téléchargement final est un malware .
- **Des campagnes à grande échelle** : Des centaines de ces sites imitant des outils populaires (comme des logiciels de nettoyage ou des utilitaires système) ont été identifiés, avec pour objectif de voler des données ou de prendre le contrôle de la machine .

C'est ici que se situe le vrai danger : un code source ouvert et légitime sur GitHub, mais distribué via un site tiers malveillant, devient un vecteur d'attaque.

🔐 **Le code source ouvert : une force, pas une faiblesse**

Contrairement à l'intuition, la licence libre (GNU) qui rend le code accessible est un atout majeur pour la sécurité.

- **La transparence** : Le code étant public, des milliers de développeurs à travers le monde peuvent l'inspecter, trouver des failles de sécurité et proposer des correctifs . C'est le

principe de "la sécurité par la transparence", par opposition à la "sécurité par l'obscurité" (le code fermé de Windows).

- **La réactivité** : Quand une vulnérabilité est découverte (comme c'est le cas pour tous les logiciels, libres ou propriétaires), elle peut être corrigée rapidement. C'est ce qui permet la publication rapide de mises à jour de sécurité.
- **La vérification par la communauté** : Il est important de noter que, même si la théorie est idéale, la réalité est plus nuancée. Le code n'est pas toujours audité en profondeur. Cependant, le système de dépôts et la réactivité de la communauté restent une protection bien plus solide que le téléchargement aléatoire de fichiers `.exe` depuis des sites non vérifiés .

🛡️ Conclusion et conseils pratiques

Votre question touche à une réalité importante : **la sécurité d'un logiciel libre ne dépend pas de sa licence, mais de la fiabilité de sa source de téléchargement.**

- **Sous Linux**, vous êtes protégé par le système de dépôts. Les risques sont bien moindres, car vous téléchargez depuis des sources officielles et vérifiées.
- **Sous Windows**, le danger est réel à cause de la prolifération de faux sites de téléchargement. Le fait qu'un programme soit open source n'offre aucune garantie sur le site qui le distribue.

Ce qu'il faut retenir pour rester en sécurité :

- **Privilégiez toujours les sources officielles** : Pour Windows, téléchargez vos logiciels uniquement depuis le site du développeur ou son dépôt officiel (ex: GitHub), jamais depuis des sites tiers de téléchargement .
- **Soyez méfiant** : Vérifiez scrupuleusement l'adresse URL du site de téléchargement. Les fraudeurs utilisent des noms de domaine très proches de l'original .
- **Mettez à jour vos logiciels** : Que vous soyez sur Linux ou Windows, appliquer les mises à jour est le geste le plus important pour vous protéger des vulnérabilités connues .