# 5 langages informatiques qui introduisent des vulnérabilités de sécurité

Même en développant dans les règles de l'art de la sécurité, un développeur peut introduire des vulnérabilités dans ses programmes. Car **les langages de programmation** sont eux-mêmes remplis de failles.

C'est du moins ce qu'avance Fernando Arnaboldi. Le chercheur en sécurité pour IOActive (cabinet américain de conseil et audit en sécurité IT ) a profité de la conférence Black Hat Europe organisé la semaine dernière à Londres pour mettre en évidence les risques induits à travers cinq langages de programmation : JavaScript, Perl, PHP, Python et Ruby. Ou, plus précisément, leurs interpréteurs exploités par nombre de logiciels, à commencer par les navigateurs.

*« Les assaillants peuvent cibler les failles de ces langages pour modifier le comportement des applications*, écrit le consultant dans son rapport. *Cela signifie que les application ne sont pas plus sécurisées que les interpréteurs des langages du code. »*

## Des problèmes inattendus de sécurité

Dans son document, le chercheur fournit des exemples concrets identifiant comment des fonctions non documentées peuvent autoriser des exécutions de commandes systèmes. Ou encore le risque que des contenus de fichiers sensibles soient exposés dans des messages d'erreur.

Sans oublier l'interprétation inattendue de code natif ou l'utilisation de noms des constantes comme chaînes de caractères régulières pour l'exécution des commandes système. Soit *« les vulnérabilités les plus graves trouvées pour chaque langage ».*

Pour mettre en avant *« ces problèmes inattendus de sécurité quand certaines fonctionnalités de langage de programmation sont utilisées »*, Fernando Arnaboldi s'est appuyé sur XDIFF, un framework de « brouillage différentiel » (differential fuzzing framework) spécialement développé pour l'occasion.

Disponible sous environnements Windows, macOS, Linux et FreeBSD, l'outil est livré en Open Source. Dans le but de faciliter la correction des vulnérabilités des langages de programmation.

---

**Lire également**
**Le navigateur Tor mise sur le langage sécurisé Rust**
**Rust 1.0 : le langage de programmation des projets critiques**
**De l'analytique à la modernisation de code : les opportunités en programmation**