Offre n°2024-08172

PhD Position F/M Quantification of security vulnerabilities caused by heavy code reuse through package managers and library dependencies

Le descriptif de l'offre ci-dessous est en Anglais

Type de contrat : CDD

Niveau de diplôme exigé : Bac + 5 ou équivalent

Fonction : Doctorant

A propos du centre ou de la direction fonctionnelle

The Inria University of Lille centre, created in 2008, employs 360 people including 305 scientists in 15 research teams. Recognised for its strong involvement in the socio-economic development of the Hauts-De-France region, the Inria University of Lille centre pursues a close relationship with large companies and SMEs. By promoting synergies between researchers and industrialists, Inria participates in the transfer of skills and expertise in digital technologies and provides access to the best European and international research for the benefit of innovation and companies, particularly in the region.

For more than 10 years, the Inria University of Lille centre has been located at the heart of Lille's university and scientific ecosystem, as well as at the heart of Frenchtech, with a technology showroom based on Avenue de Bretagne in Lille, on the EuraTechnologies site of economic excellence dedicated to information and communication technologies (ICT).

Contexte et atouts du poste

The doctoral project is part of the SWHSec project. It will be supervised by Clémentine Maurice and Pierre Laperdrix, both CNRS researcher in the Spirals team.

The objective of the SWHSec project is to explore several of the new possibilities offered by the availability of Software Heritage to blend together the "vertical" and "horizontal" approaches to software supply chain security.

The research will be conducted in the Spirals team.

Mission confiée

Package managers like Maven, npm or Yarn are widely used today to simplify software development. By writing a few lines in a configuration file, a developer can import code from many different projects to build an application. However, any vulnerability in an imported package can compromise the security of an entire application and can even propagate to an entire infrastructure.
Overall, our aim here is to understand the prevalence of vulnerabilities in packages from package managers and see how much impact one vulnerability can cause. By analyzing the code stored by Software Heritage and linking it to a vulnerability database like Snyk.io, it will be possible to understand at a very large scale how package managers can create security vulnerabilities in software around the world.

The first step for the PhD student will be to build a synthetic state of the art regarding existing empirical studies on the prevalence of flows in open-source package repositories. We will also investigate in detail two known incidents already reported in the past where one single package affected the security of entire applications, like with the event-stream incident in the npm ecosystem or log4j. Another example of compromise in this task is the use of cryptographic libraries where one vulnerable version can compromise the integrity of encrypted connections.

From these first studies, the goal is to explore how we could detect a set of patterns applicable to Software Heritage allowing developers to observe risks in an open source ecosystem. The idea, as far as possible, is to propose a risk metric for each dependency with respect to the security of the global ecosystem.

Principales activités

- Bibliography on software supply chain attacks,
- Propose and implement techniques to understand the effect of a vulnerability in a package on all its dependencies,
- Scientific publications in top international conferences,
- Presentations of the work in national and international conferences, and in project meetings.

Compétences

The ideal candidate will have the following skills:

- Good mastery of English
- Good programming skills and supporting tools.
- Relational skills, e.g., working in a team, effective reporting and communication with all involved stakeholders.
- Sound background in computer science, including machine learning, graphs, and security.

Avantages

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

Informations générales

- **Thème/Domaine :** Sécurité et confidentialité
  Systèmes d'information (BAP E)
- **Ville :** Villeneuve d'Ascq
- **Centre Inria :** Centre Inria de l'Université de Lille
- **Date de prise de fonction souhaitée :** 2024-11-01
- **Durée de contrat :** 3 ans
- **Date limite pour postuler :** 2025-07-05

Contacts

- **Équipe Inria :** SPIRALS
- **Directeur de thèse :**
  Maurice Clémentine / clementine.maurice@inria.fr

A propos d'Inria

Inria est l'institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2600 personnes. Ses 215 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3900 scientifiques pour relever les défis du numérique, souvent à l'interface d'autres disciplines. L'institut fait appel à de nombreux talents dans plus d'une quarantaine de métiers différents. 900 personnels d'appui à la recherche et à l'innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 200 start-up. L'institut s'e?orce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

Attention: Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.

Consignes pour postuler

Please send your CV and Cover letter.

Sécurité défense :
Ce poste est susceptible d'être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L'autorisation d'accès à une zone est délivrée par le chef d'établissement, après avis ministériel favorable, tel que défini dans l'arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l'annulation du recrutement.

Politique de recrutement :
Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.