Offer #2024-08172

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

Contract type : Fixed-term contract

Level of qualifications required : Graduate degree or equivalent

Fonction : PhD Position

About the research centre or Inria department

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).

Context

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.

Assignment

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.

Main activities

- 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.

Skills

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.

Benefits package

- 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

General Information

- **Theme/Domain :** Security and Confidentiality
  Information system (BAP E)
- **Town/city :** Villeneuve d'Ascq
- **Inria Center :** Centre Inria de l'Université de Lille
- **Starting date :** 2024-11-01
- **Duration of contract :** 3 years
- **Deadline to apply :** 2025-07-05

Contacts

- **Inria Team :** SPIRALS
- **PhD Supervisor :**
  Maurice Clémentine / clementine.maurice@inria.fr

About Inria

Inria is the French national research institute dedicated to digital science and technology. It employs 2,600 people. Its 200 agile project teams, generally run jointly with academic partners, include more than 3,500 scientists and engineers working to meet the challenges of digital technology, often at the interface with other disciplines. The Institute also employs numerous talents in over forty different professions. 900 research support staff contribute to the preparation and development of scientific and entrepreneurial projects that have a worldwide impact.

Warning : you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.

Instruction to apply

Please send your CV and Cover letter.

Defence Security :
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST).Authorisation to enter an area is granted by the director of the unit,

following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

Recruitment Policy :
As part of its diversity policy, all Inria positions are accessible to people with disabilities.