

Bachelor-/Masterarbeit

Schwachstellenbewertung in der Software-Supply-Chain

Ziel

Moderne Software besteht zu großen Teilen aus Fremdkomponenten, für die laufend neue Schwachstellen veröffentlicht werden: in CVE-Datenbanken (CVE/NVD, OSV), Hersteller-Advisories oder Write-ups von Sicherheitsforschenden. Bestehende Werkzeuge melden jedoch viele Schwachstellen, die im konkreten Produkt gar nicht ausnutzbar sind, etwa weil der verwundbare Code nicht einkompiliert, nie aufgerufen oder von außen nicht erreichbar ist.

Ziel dieser Arbeit ist es, für ein gegebenes Projekt (z. B. Web-Anwendung oder Embedded-Firmware) Schwachstelleninformationen aus verschiedenen Quellen zusammenzuführen und zu prüfen, ob sie das **finale Produkt tatsächlich betreffen**, also ausnutzbar sind. Methodisch ist die Arbeit offen: Neben statischer und dynamischer Analyse können auch LLMs bzw. Agenten eingesetzt werden. Das genaue Thema wird nach Absprache festgelegt. Mögliche Schwerpunkte:

- Zusammenführung heterogener Schwachstellenquellen
- Reachability-Analyse des verwundbaren Codes
- Konfigurations- und Build-Analyse für Embedded-Systeme
- Automatisierte Erstellung von VEX-Aussagen (Vulnerability Exploitability eXchange)

Anforderungen und Voraussetzungen

- Einarbeitung in Supply-Chain-Security, SBOMs und Schwachstellendatenbanken
- Konzeption und prototypische Implementierung eines Bewertungsverfahrens
- Evaluation an realen Projekten und Vergleich mit bestehenden Werkzeugen
- Programmierkenntnisse (z. B. Python), Linux-Erfahrung und Interesse an IT-Sicherheit

Ansprechpartner

Prof. Dr. Lothar Braun | ✉ lothar.braun@tha.de | ☎ +49 821 5586-3378

THA_innos

Das Institut für innovative Sicherheit (THA_innos) bietet eine Vielzahl von Abschluss- und Projektarbeiten im Themenfeld der Cyber Security an. Unser Team unterstützt Studierende dabei mit Know-How und Praxiserfahrung und ist zudem offen für eigene Themenvorschläge. Durch die enge Zusammenarbeit mit der Forschungsgruppe vor Ort im MRM-Gebäude lernen Studierende sowohl das Institutsleben, als auch die aktuelle Forschung von THA_innos kennen.

Weitere Informationen auch unter <https://innos.tha.de>