MITRE'S Hipcheck AUTOMATES SOFTWARE SUPPLY CHAIN RISK ASSESSMENT

Hipcheck is a tool for automated assessment of supply chain risk for software. It identifies high risk software by analyzing project history, metadata, contents, and contributors, and guides further manual review.

Need for Hipcheck

Software supply chain security is an important challenge; software projects benefit from open source components but take on risks associated with vulnerabilities in, or attacks against, those components. Auditing dependencies is a best practice, but the time and effort required can be enormous, and new versions must be audited with each release.

Benefits

Hipcheck assesses the practices used to produce software and detects possible attacks against a software repository.

Beyond detecting known vulnerable versions, Hipcheck understands whether projects practice secure development and are actively maintained, whether the contributors can be trusted, and more.

Hipcheck helps thwart attacks by finding possible malicious contributions, where vulnerabilities are introduced by seemingly benign changes, and typosquatting attacks where attackers create malicious packages whose names are similar to legitimate packages.

- Hipcheck's "pass/investigate" determinations make it possible for projects to focus their supply chain analysis on high-risk packages.
- Hipcheck can be deployed in an automated or manual fashion, including in Continuous Integration pipelines or as part of a software onboarding process.
- It is fully configurable, allowing users to set thresholds, set weights for individual analyses, and define their overall risk tolerance.
- Default configurations are set based on real-world analysis of open source repositories, providing confidence that risky dependencies will be flagged.
- Hipcheck is high-performance, analyzing even extremely large repositories in a few minutes to produce actionable determinations.

Competitive Advantage

Hipcheck can be used to expand commercial software supply chain security solutions. Existing solutions can leverage Hipcheck's analytics to amplify their product's ability to identify high-risk practices and possible supply chain attacks.

Licensing Opportunities

The MITRE Corporation is seeking licensees for commercial development of Hipcheck. Hipcheck has been demonstrated in laboratory settings and active government programs and is available for use by industry through MITRE's licensing program.

Hipcheck makes managing software supply chain risk possible at scale.

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

For more information, please contact:
techtransfer@mitre.org

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®