ABSTRAK

PENGEMBANGAN *FRAMEWORK* ASESMEN DAMPAK PERAMBATAN *VULNERABILITY* PADA NODE PACKAGE MANAGER (NPM)

Putra Perdana Haryana
15/383250/PA/16910

Node Package Manager (npm) adalah sebuah layanan *package repository* yang menopang keberlangsungan ekosistem Node.js secara khusus dan JavaScript secara umum. Sebagai repositori yang bersifat *open source*, npm memungkinkan siapapun untuk memublikasikan *package* karyanya agar dapat dimanfaatkan oleh orang lain tanpa ada proses *screening*. Hal tersebut, ditambah praktik *code reuse* (penggunaan bagian kode dari perangkat lunak lain) yang sangat umum di kalangan pengembang perangkat lunak, membuka jalan bagi *vulnerability* yang dimuat oleh suatu *package* untuk merambat ke *package* lain melalui jaringan *dependency*.

Pada penelitian ini akan dikembangkan *framework* identifikasi *package* pewaris *vulnerability* di jaringan *dependency* antar-*package* npm. Proses identifikasi mengadopsi pendekatan temporal agar alur evolusi *package* menjadi perhatian. Pendekatan komputasi *big data* diterapkan untuk mengakomodasi besarnya ukuran *dataset* jaringan npm.

Framework diaplikasikan untuk melakukan asesmen pada *dataset snapshot* npm pada tanggal 2 November 2017 dan laporan *advisory* snyk.io hingga tanggal 9 November 2017. Dari 267 *package* yang dilaporkan memuat *vulnerability*, *framework* berhasil mengidentifikasi sebanyak 187.694 *package* terdampak yang tersebar hingga pada 13 level kedalaman *dependency*. Hasil asesmen pada studi ini dapat dijadikan gambaran umum bagi pengembang perangkat lunak untuk mencegah risiko perambatan *vulnerability*.

Kata kunci: npm, perambatan *vulnerability*, jaringan *dependency*

ABSTRACT

DEVELOPMENT OF ASSESMENT FRAMEWORK ON THE EFFECT OF VULNERABILITY PROPAGATION IN THE NODE PACKAGE MANAGER (NPM)

Putra Perdana Haryana
15/383250/PA/16910

Node Package Manager (npm) is a package repository service that supports the Node.js and JavaScript ecosystem. Being an open-source project, it allows everyone to publish their package to be used by anyone else without any screening procedure. With code reuse being a very common practice among software developers, it paves the path for vulnerabilities to propagate among packages in the dependency network.

This study aims to develop a framework to identify vulnerability propagation in transitively-dependent packages along the dependency network. Identification process adopts temporal approach to put more focus on package evolution. Big data computational approach is applied to accomodate the sheer size of whole npm ecosystem data.

The framework is then applied to assess the npm snapshot of November 2 2017 with snyk.io's advisory report until November 9 2017. From the initial 267 reportedly vulnerable packages, the framework identified 187.694 affected packages up to 13 dependency-level deep. This finding may give software developers a big picture on the security state of the npm ecosystem to anticipate vulnerability propagation risk.

Keywords: npm, vulnerability propagation, dependency network