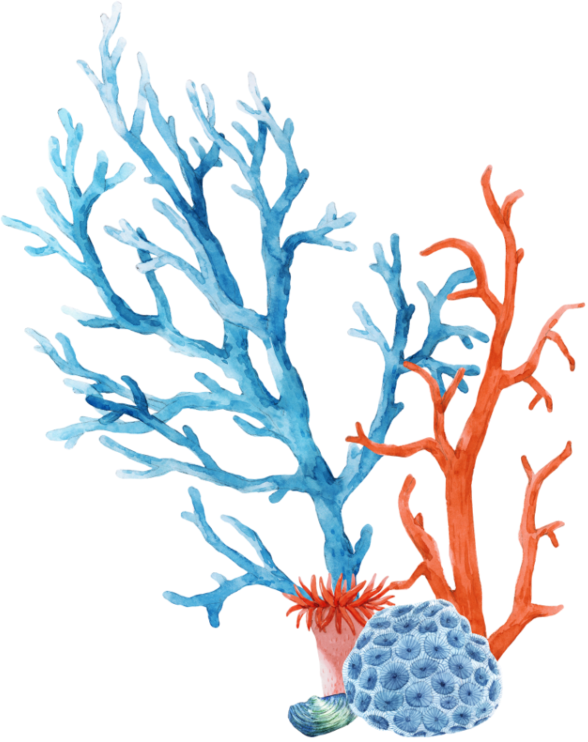
Node.js Secure Coding

Defending Against Command Injection Vulnerabilities



LIRAN TAL

Node.js Secure Coding: Defending Against Command Injection Vulnerabilities

Liran Tal

Version v1.1, 01.05.2023:

Table of Contents

Node.js Secure Coding: Defending Against Command Injection Vulnerabilities
by Liran Tal

Revision history:

1. 2023-05-01
    1. New Appendix chapter includes self-assessment questions, reviews of closed-source and open-source real-world command injection vulnerability implications, and CVE list.
    2. Chapter 2: Argument Injection features citation of prior research.
2. 2023-04-07
    1. First edition.

This book is for sale at https://www.nodejs-security.com

Preface

Learn about secure coding practices with Node.js based on real-world CVE vulnerabilities in popular open-source npm packages.

This book takes an adventure-based approach to application security learning, where you will be playing detective who unravels the mysteries of common security vulnerabilities. Through these exercises you will learn about secure coding practices, and how to avoid security pitfalls that software developers and open-source maintainers get caught with.

Senior software engineers often recite how one of the most critical skills you should have as an engineer is the ability to read code. The more you read, the easier it becomes for you to understand code and the more context you gain. This book focuses exactly on that - reading vulnerable code, so we can learn from it. This activity creates patterns that our brain learns to identify and that later quickly turn into red flags that we detect and apply in our day-to-day programming and code review routines.

What you gain to learn

Designed for software developers and security professionals interested in command injection, this book provides a comprehensive understanding of the topic. It also demonstrates its impact and concerns on web application security.

Through insecure coding practices found in vulnerable open-source npm packages, this book examines the security aspects affecting JavaScript and Node.js applications. Developers of other languages such as Python will find references to insecure code and best practices relatively easy to transfer to other server-side languages and software ecosystems.

By completing this book you stand to gain:

- A high level of security expertise on the topic of command injection vulnerabilities.
- An understanding of application security jargon and conventions associated with security vulnerabilities management and severity classification.
- How real-world software libraries were found to be vulnerable and their methods of fixing security issues.
- Adopting a security-first mindset to recognize patterns of insecure code.
- Secure coding best practices to avoid command injection security vulnerabilities.

- Proficiency in performing secure code reviews as they apply to concerns and the scope of command injection security vulnerabilities.

Software developers

Software developers who build web applications, and specifically those who practice server-side JavaScript development on-top of the Node.js runtime will greatly benefit from the secure coding practices learned in this book.

As a software developer, you will engage in step-by-step code review of real-world popular libraries and their vulnerable code, through which you will investigate how security vulnerabilities manifest and understand the core reasons that lead to a security risk.

By reviewing code used in real-world software libraries, you will learn to recognize patterns of insecure code. In addition, you will learn secure coding best practices for working with system processes.

Security practitioners

Security professionals who wish to learn and investigate the source of insecure code and security implications concerned with vulnerable open-source and third-party libraries that make up an application's software composition analysis (SCA).

How to read this book?

This book primarily focuses on the following knowledge-base sections:

- Introduction to application security
- A primer on command injection
- Chapters that review security vulnerabilities in-depth

If you have a high level of familiarity and understanding of application security concepts such as OWASP, NVD, and other security jargon then you can skip the ***Introduction to application security concepts***.

For readers who have an in-depth understanding of command injection vulnerabilities, such as those who have prior experience fixing them as a developer, or disclosing a command injection vulnerability through a bug bounty program, you can skip the command injection primer. Keep in mind, the command injection introduction chapter provides an elaborate foundation of different types and other insightful security considerations. It can still be effective educational content even for experienced practitioners.

At the core of this book is a deep-dive into real-world security vulnerabilities reviews. Each vulnerability that we review is assigned a security identifier, such as a CVE, and has impacted real-world npm packages, some of which you might even be using.

About the Author

Liran Tal is an accomplished software developer, respected security researcher, and prominent advocate for open-source software in the JavaScript community. He has earned recognition as a ***GitHub Star***, in part for his tireless efforts to educate developers and for his contributions to developing essential security tools and resources that help JavaScript and Node.js developers create more secure applications.

His leadership in open-source security extends to meaningful contributions to OWASP projects, recording supply chain security incidents at the CNCF, and various OpenSSF initiatives. His contributions to the Node.js community have been widely recognized, including being honored with the ***OpenJS Foundation's Pathfinder for Security award*** for his significant contributions to advance the state of Node.js security. In his role as a security analyst in the Node.js Foundation's Security Working Group, Liran reviewed hundreds of vulnerability reports for npm packages and created processes for responsible security disclosures and vulnerability triage.

Liran is also an accomplished security researcher and has disclosed security vulnerabilities in various open-source software projects, including being credited with CVEs impacting npm packages. His work on supply chain security research, including Lockfile Injection, was presented at Black Hat Europe 2021 cybersecurity conference.

As an experienced author and educator, Liran has written several widely respected books on software security. These include "Serverless Security" published by O'Reilly, as well as the self-published titles "Essential Node.js Security" and "Web Security: Learning HTTP Security Headers". He is passionate about sharing his knowledge and occasionally speaks on software security topics at academic institutions, such as presenting to students at the Electrical and Computer Engineering School at Purdue University.

Since joining Snyk, Liran has made a significant impact as a developer advocate, empowering developers with the knowledge and tools needed to build and deploy secure software at scale. His contributions to the developer community have been instrumental in advancing the state of application security and strengthening the adoption of secure coding practices.

Chapter 1

Introduction to Application Security

It’s necessary for software developers to understand the terminology used by security professionals, become aware of their standards and comprehend the role they play in application security. Doing so can assist in assimilating information on secure coding, which is a fundamental component of IT security.

Learnings

By the end of this chapter, you should be able to answer questions such as:

- What is a CVE and how is a CWE related to it?
- What is the OWASP Top 10?
- What is NVD?
- What is a source-to-sink?
- What is an attack vector?