M.A.C.K.
Memory Leak
Sprint 4 Security Evaluation

Prepared by Andrew Palmer

Capstone Project: Spring 2022

The University of West Florida

Last Modified:

28 April 2022

CIS4595: Capstone Project

Dr. Bernd Owsnicki Klewe

Table of Contents

```
andrewpalmer@Andrews-MacBook-Pro memory_leak % npm audit fix

changed 3 packages, and audited 1188 packages in 2s

102 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities
```

1. Introduction

All tests were performed on the application that was being hosted by Firebase. All attempted exploits and attacks were performed in such a way that a success would not impact the status of the server or database in any negative or irreversible way. For this evaluation, there were few applicable attacks that I was able to execute due to the application not having all functionalities implemented. In future evaluations, it is likely that more potential exploits and vulnerabilities will be included since there will be more functionality to evaluate.

2. Attempted Exploits/Attacks

a. Cross-site Scripting - *failed*

   i. The results of this test are the same as the previous two evaluations.

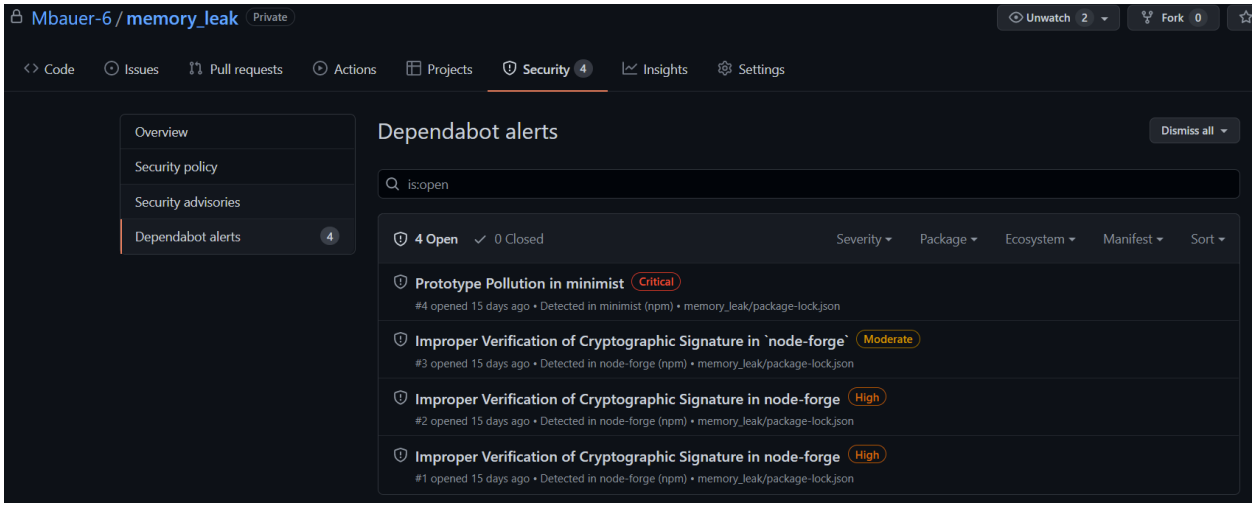
b. DOM-based XSS - *failed*

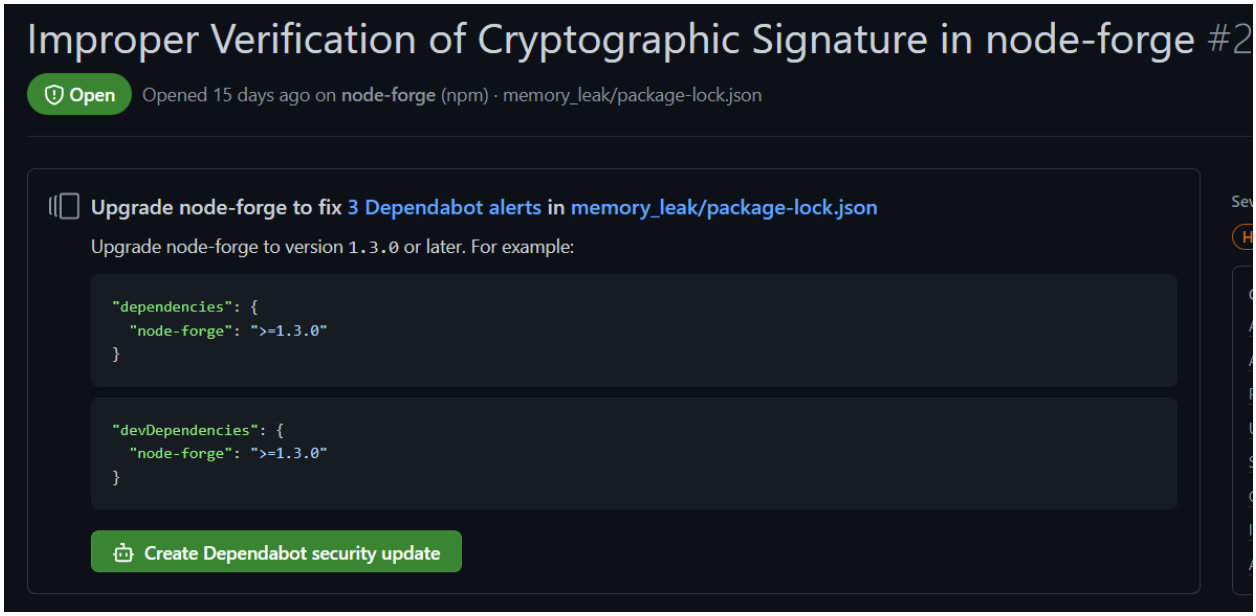
   i. The results of this test are the same as the previous two evaluations.

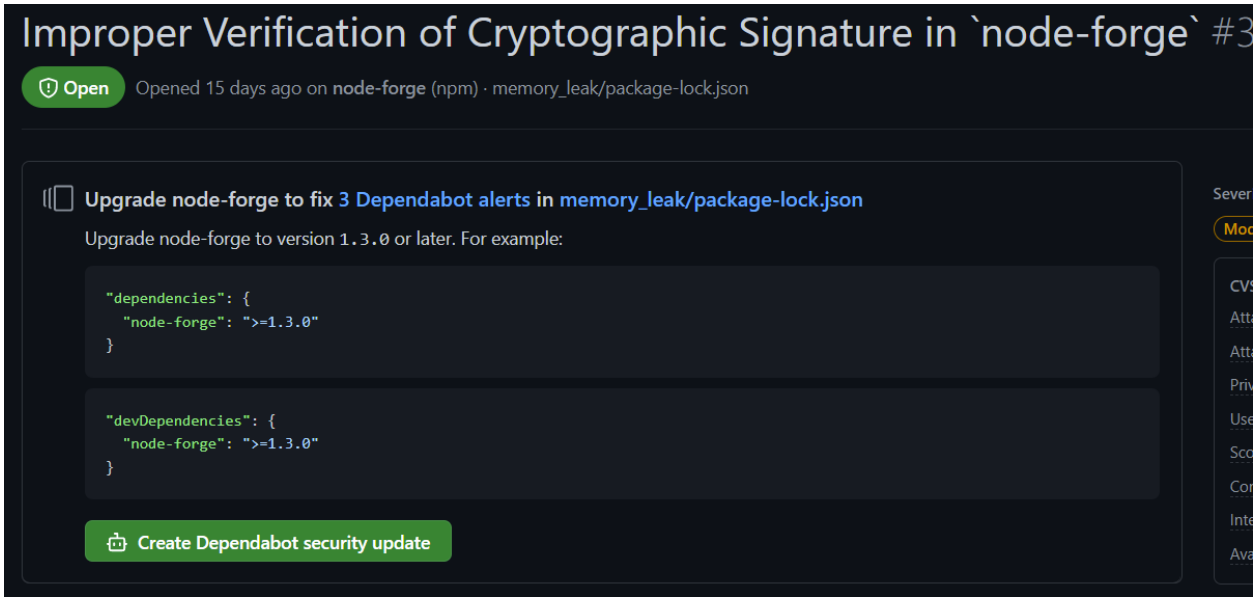
3. Codebase Vulnerabilities

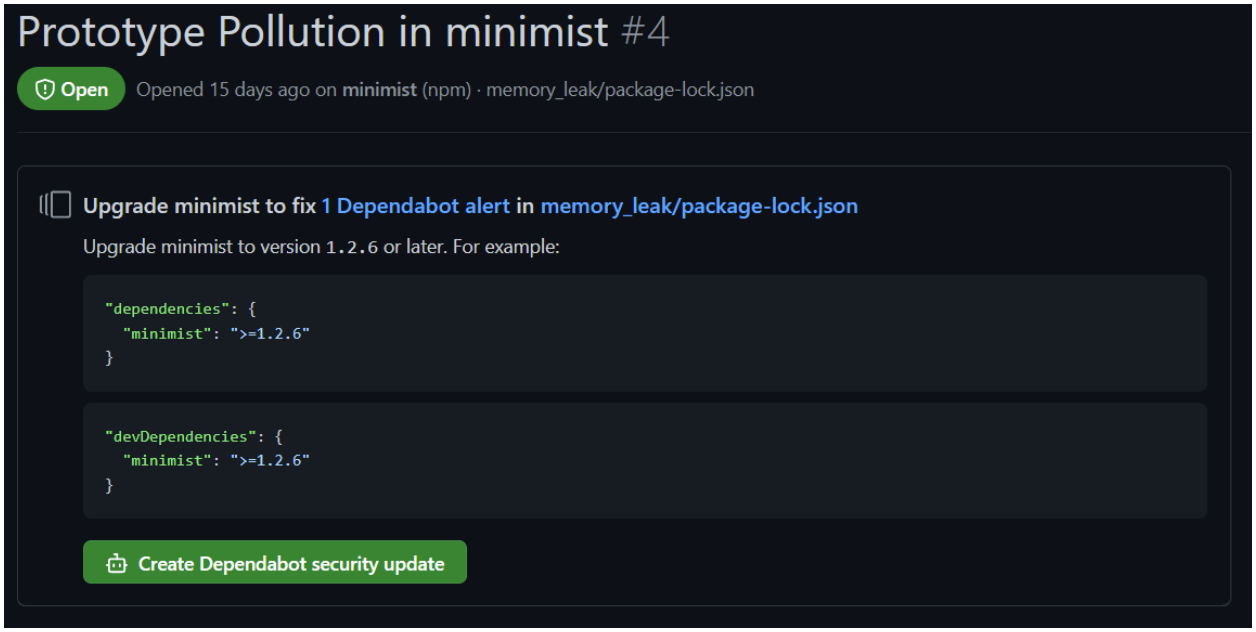
GitHub's dependabot alerts feature informed us of security vulnerabilities that were present in our package-lock.json, indicating that we had out-of-date

dependencies in our project. The packages that needed to be addressed were minimist and node-forge.




Improper Verification of Cryptographic Signature in node-forge #2
Open
Opened 15 days ago on node-forge (npm) · memory_leak/package-lock.json
Upgrade node-forge to fix 3 Dependabot alerts in memory_leak/package-lock.json
Upgrade node-forge to version 1.3.0 or later. For example:
"dependencies": {
"node-forge": ">=1.3.0"
}
"devDependencies": {
"node-forge": ">=1.3.0"
}
Create Dependabot security update


Improper Verification of Cryptographic Signature in `node-forge` #3
Open
Opened 15 days ago on node-forge (npm) · memory_leak/package-lock.json
Upgrade node-forge to fix 3 Dependabot alerts in memory_leak/package-lock.json
Upgrade node-forge to version 1.3.0 or later. For example:
"dependencies": {
"node-forge": ">=1.3.0"
}
"devDependencies": {
"node-forge": ">=1.3.0"
}
Create Dependabot security update



To remediate these vulnerabilities, I updated the versions of minimist and node-forge to their latest version. These are 1.2.6 and 1.3.1, respectively.

```
andrewpalmer@Andrews-MacBook-Pro memory_leak % npm install minimist@latest

removed 2 packages, changed 3 packages, and audited 1188 packages in 3s

102 packages are looking for funding
  run `npm fund` for details

2 high severity vulnerabilities

To address all issues, run:
  npm audit fix

Run `npm audit` for details.
```

```
andrewpalmer@Andrews-MacBook-Pro memory_leak % npm install node-forge@latest

changed 1 package, and audited 1188 packages in 3s

102 packages are looking for funding
  run `npm fund` for details

1 high severity vulnerability

To address all issues, run:
  npm audit fix

Run `npm audit` for details.
```

After updating these two packages, npm audit reported more vulnerabilities, which were remediated using an npm audit fix command. After this step, no vulnerabilities were reported either by npm or GitHub.

```
andrewpalmer@Andrews-MacBook-Pro memory_leak % npm audit
# npm audit report

async  <2.6.4
Severity: high
Prototype Pollution in async - https://github.com/advisories/GHSA-fwr7-v2mv-hh
fix available via `npm audit fix`
node_modules/async

1 high severity vulnerability

To address all issues, run:
  npm audit fix
```

```
andrewpalmer@Andrews-MacBook-Pro memory_leak % npm audit fix

changed 1 package, and audited 1188 packages in 4s

102 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities
```