

Open Source Engineer Task

Welcome future Sealer!

We just found out that Penguin Software Inc., one of our biggest clients, is using a vulnerable package and looking for us to save the day.

As part of their web application written in Node.JS, Penguin uses `tough-cookie` 2.5.0 to process their clients' cookies. Unfortunately, it is affected by [CVE-2023-26136](#), rated as a critical vulnerability by NIST's NVD.

According to the vulnerability advisory, the only way to solve the issue is by upgrading to 4.1.3. However, the Penguins feel shorthanded (pun intended) and don't have the necessary capacity to adjust their code to work with the new version of `tough-cookie`.

In order to help them, our goal is to create a customized version of `tough-cookie` 2.5.0 which is not vulnerable to CVE-2023-26136.

What do we expect from you?

1. Packed version of the patched `tough-cookie` 2.5.0 in `.tgz` format (you can use `npm pack` to generate it). Notice that:
 - a) It should be identical to the public version except for your changes.
 - b) The `test suite` should **pass** - please include the command you used to run the tests and its output.
 - c) Include a unit-test to verify the vulnerable behavior was fixed.
2. A `changes.diff` file with your changes compared to the `tough-cookie` 2.5.0 git tag. You should be able to apply the file to the cloned code using `git apply changes.diff`. Please ensure no unintended changes are included.

3. An `index.js` file exploiting the vulnerability. Notice that:
 - a) After running `npm install tough-cookie@2.5.0 && node index.js` the output should contain `EXPLOITED SUCCESSFULLY`
 - b) After running `npm install ./tough-cookie-2.5.0-PATCHED.tgz && node index.js` the output should be `EXPLOIT FAILED`.
 - c) Include comments explaining the triggered vulnerability and the potential damage.
 - d) It should be running on Node 20 (LTS).
4. A link to your [forked GitHub repository](#) of `tough-cookie` 2.5.0 and a Git Tag that includes your changes.
5. A list of all the CI (Continuous Integration) tools you have used in the past and your level of expertise with each.

Please note that artifacts from items 1-3 may be blocked by your email. Therefore, upload them to a file-sharing service (like Google Drive) and share a link that is accessible to everyone.

If you have any questions - feel free to reach out to jobs-questions@sealsecurity.io

Good Luck!