ReDoS in Node.js

Alexandru Olaru
@alxolr
alxolr.com

What is ReDoS

- is an **algorithmic complexity attack** that produces a **denial-of-service** by providing a regular expression that takes a very long time to evaluate.
- the **time** taken can **grow exponentially** in relation to input size

Examples of vulnerable regexes

- `/(a+)+/`
- `/([a-zA-Z]+)*/`
- `/(a|aa)+/`
- `/(a|a?)+/`
- `/(.*a){x}/ for x > 10`

- the regular expression applies repetition ("+", "*") to a complex subexpression;
- for the repeated subexpression, there exists a match which is also a suffix of another valid match.

Mitigation techniques

- https://www.owasp.org/index.php/OWASP_Validation_Regex_Repository
- Never write your own regexes use validate.js or any other validation library
- Use look aheads ?= to create atomic groups

- Use redosy to identify existing vulnerable regexes

```
npm install -g redosy
redosy /path/to/your/project
```

References

- https://medium.com/@liran.tal/node-js-pitfalls-how-a-regex-can-bring-your-system-down-cbf1dc6c4e02
- https://snyk.io/blog/redos-and-catastrophic-backtracking/
- https://en.wikipedia.org/wiki/ReDoS
- https://github.com/alxolr/redosy - npm package to scan for regex denial vulnerabilities
- 0x - node.js profiling tool