Electronegativity

Identify misconfigurations and security anti-patterns in Electron applications.

Lorenzo Stella @ Doyensec
Arsenal Station 1, August 7, from 4:00 pm to 5:20 pm
Try it now!

Available on:

https://github.com/doyensec/electronegativity

$ npm install @doyensec/electronegativity -g
Electron... what?
The Electron Stack

![Chrome Icon](image)

+ 

![JavaScript Icon](image)
...and many others!
Security Audits on Electron Applications

• Large Attack Surface
  Custom code, Dependencies, Electron Framework APIs and Foundation Libraries (Chromium/NodeJS)

• Rapidly Ever-Changing Framework Security
  Frequent security patches, recent nodeIntegration bypasses or attacks, best webPreferences settings are always evolving.

• Lots of Things to Check
  Electron Security Checklist by @ikkisoft, traditional web vulnerabilities, risky security anti-patterns, hardening best practices
How Do You Survive Through This?

**Electronegativity** can help you!

- Statically analyzes the code using AST and DOM parsing
- Looks for security-relevant Electron configurations
- Includes all the checks from the Electron Security Checklist (more than 40 and counting!)
- Checks if the Electron version used is vulnerable
- Suggests secure coding practices
- ...and much more!
Usage

• Using it is as simple as pointing it to the repository directory or to the final .asar package.
Versatile Checks System
Supported checks

- Affinity Global Check
- Allow Popup Check
- Auxclick JS/HTML Check
- Available Security Fixes Global Check
- Blink Features JS/HTML Check
- Certificate Error Event JS Check
- Certificate Verify Proc JS Check
- Context Isolation JS Check
- Custom Arguments JS/JSON Check
- CSP Global Check
- Dangerous Functions JS Check
- Electron Version JSON Check
- Experimental Features JS/HTML Check
- HTTP Resources JS/HTML Check
- Insecure Content JS/HTML Check
- Limit Navigation JS Check
- Node Integration JS/HTML Check
- Node Integration Attach Event JS Check
- Open External JS Check
- Permission Request Handler JS Check
- Preload JS Check
- Protocol Handlers JS Check
- Sandbox JS Check
- Security Warnings Disabled JS/JSON Check
- Web Security JS/HTML Check

...and more to come!
CSV and Sarif Output Formats

doyensec $ electronegativity -i /tmp/electropositivity --output results.csv
Demo Time: Electronegativity & Insecure Preload Detection

- Wire Arbitrary File Write via Insecure Preload
- Discord Arbitrary IPC via Insecure Preload

...Or
Discord Arbitrary IPC via Insecure Preload
Electronegativity can help you detect this! (thanks to a dedicated PRELOAD_JS_CHECK)
Grab your copy today!

$ npm install @doyensec/electronegativity -g

Questions?
(lorenzo@doyensec.com)