steveukx / **git-js** Public

Code | Issues 48 | Pull requests 7 | Actions | Security and quality 2 | Ir

Commit 89a2294

steveukx authored 2 weeks ago · ✓ 8 / 8 · Verified

```
Environment Parsing (#1156)

* Apply unsafe filtering for `--template` flag, vulnerable merge config and setting config by
environment variable
* Adds `diff.textconv`, `filter.clean` and `filter.smudge` to known exploitable `git config`
operations.
* Add environment variable scanning to unsafe plugin
* Extend vulnerability scanning to additional filters, gpg and more configuration options
* Update documentation for unsafe plugin
```

main (#1156) · simple-git@3.36.0 ••• @simple-git/args-pathspec@1.0.3

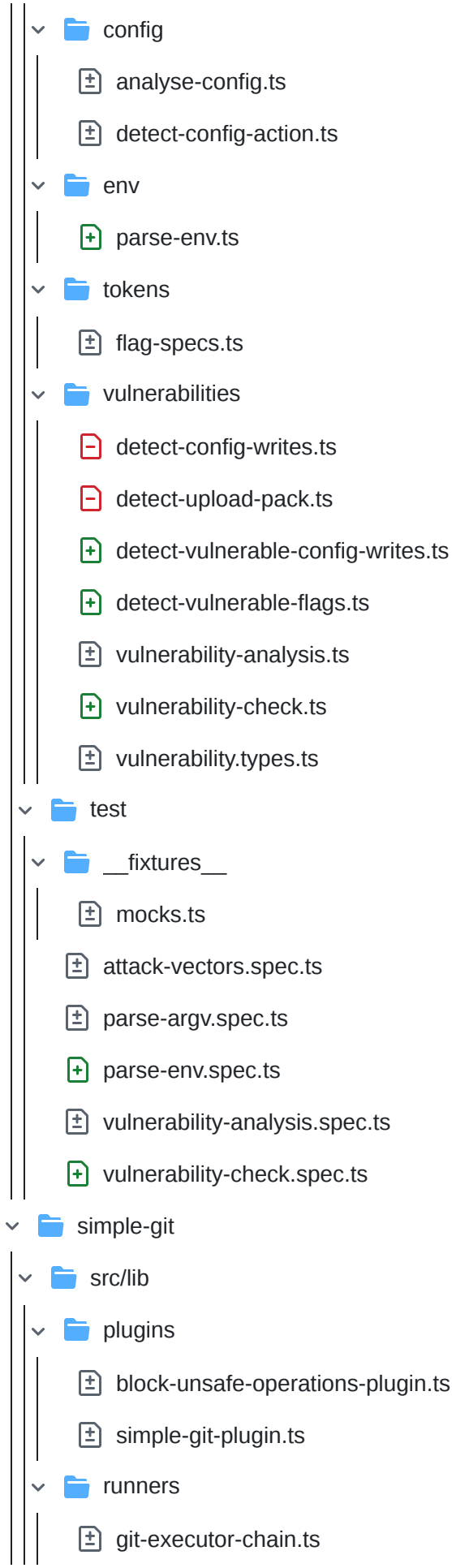
1 parent 7dd8c96 commit 89a2294

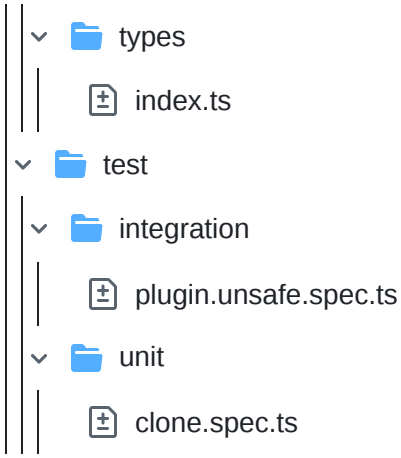
29 files changed +1,093 -279

Top

Filter files…

- .changeset
  - config.json
  - deep-ducks-care.md
- docs
  - PLUGIN-UNSAFE-ACTIONS.md
- packages/argv-parser
  - index.ts
  - src
    - args
      - parse-argv.ts
      - parse-argv.types.ts


config
analyse-config.ts
detect-config-action.ts
env
parse-env.ts
tokens
flag-specs.ts
vulnerabilities
detect-config-writes.ts
detect-upload-pack.ts
detect-vulnerable-config-writes.ts
detect-vulnerable-flags.ts
vulnerability-analysis.ts
vulnerability-check.ts
vulnerability.types.ts
test
__fixtures__
mocks.ts
attack-vectors.spec.ts
parse-argv.spec.ts
parse-env.spec.ts
vulnerability-analysis.spec.ts
vulnerability-check.spec.ts
simple-git
src/lib
plugins
block-unsafe-operations-plugin.ts
simple-git-plugin.ts
runners
git-executor-chain.ts



Search within code

.changeset/config.json

```
@@ -1,10 +1,10 @@
 {
-  "$schema": "https://unpkg.com/@changesets/config@1.6.4/schema.json",
+  "$schema": "https://unpkg.com/@changesets/config@3.1.3/schema.json",
   "changelog": "@changesets/cli/changelog",
   "commit": false,
   "linked": [],
   "access": "public",
-  "baseBranch": "main",
+  "baseBranch": "origin/main",
   "updateInternalDependencies": "patch",
   "ignore": [
     "@simple-git/test-utils"
```

.changeset/deep-ducks-care.md

```
@@ -0,0 +1,11 @@
+ ---
+ "@simple-git/argv-parser": minor
+ simple-git: minor
+ ---
+
+ Extend known exploitable configuration keys and per-task environment variables.
+
```

```
8  + Note - `ParsedVulnerabilities` from `argv-parser` is removed in favour of a
     readonly array of `Vulnerability` to match usage in `simple-git`, rolled into
     the new `vulnerabilityCheck` for simpler access to the identified issues.
9  +
10 + Thanks to @zebbern for identifying the need to block `core.fsmonitor`.
11 + Thanks to @kodareef5 for identifying the need to block `GIT_CONFIG_COUNT`
     environment variables and  `--template` / `merge` related config.
```

Comments 0

Please sign in to comment.