open-policy-agent / opa Public

Code Issues 298 Pull requests 2 Actions Projects 1 Wiki •••

Formatting generated code can change ordering of array literals

Moderate **srenatus** published **GHSA-hcw3-j74m-qc58** on Feb 9

Package

github.com/open-policy-agent/opa (Go)

Affected versions	Patched versions
>= 0.33.1	0.37.2

Description

Impact

Under certain conditions, pretty-printing an AST that contains synthetic nodes could change the logic of some statements by reordering array literals. Example of policies impacted are those that parse and compare web paths, see the example below.

All of these three conditions have to be met to create an adverse effect:

1. An AST of Rego had to be **created programmatically** such that it ends up containing terms without a location (such as wildcard variables).
2. The AST had to be **pretty-printed** using the `github.com/open-policy-agent/opa/format` package.
3. The result of the pretty-printing had to be **parsed and evaluated again** via an OPA instance using the bundles, or the Golang packages.

If any of these three conditions are not met, you are not affected.

Notably, all three would be true if using **optimized bundles**, i.e. bundles created with `opa build -O=1` or higher.
In that case, the optimizer would fulfil condition (1.), the result of that would be pretty-printed when writing the bundle to disk, fulfilling (2.). When the bundle was then used, we'd satisfy (3.).

Example

For example, the process outlined above could turn this rule

```
hello {
        ["foo", _] = split(input.resource, "/")
}
```

into

```
hello {
        [_, "foo"] = split(input.resource, "/")
}
```

with an input of

```
{
    "resource": "foo/bar"
}
```

the result would change from

```
{
    "hello": true
}
```

to (no default value of hello)

```
{}
```

The severity was determined to be *moderate* because the conditions are quite particular. Please note that its only the OPA bundle build process thats affected. An OPA sidecar of version 0.36.0 with an optimized bundle built by OPA 0.32.1 would not face this bug.

Patches

Fixed in version 0.37.2.

Workarounds

- Disabling optimization when creating bundles.

References

- Introduced in #3851
- Backported for the 0.33.1 patch release: `bfd984d`
- Fixed by `932e4ff` and `2bd8eda`

For more information

If you have any questions or comments about this advisory:

- Open an issue in Community Discussions
- Ask in Slack: https://slack.openpolicyagent.org/

Severity

Moderate

CVE ID

CVE-2022-23628

Weaknesses

No CWEs

Credits

johanneslarsson