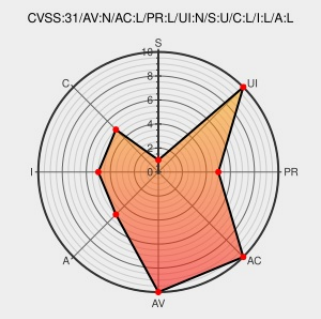
CVE-2022-23628

Published on: 02/09/2022 12:00:00 AM UTC

Last Modified on: 02/17/2022 02:37:00 AM UTC

CVE-2022-23628 - advisory for GHSA-hcw3-j74m-qc58

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Open Policy Agent from Openpolicyagent contain the following vulnerability:

OPA is an open source, general-purpose policy engine. Under certain conditions, pretty-printing an abstract syntax tree (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. **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.). As a workaround users may disable optimization when creating bundles.

CVE-2022-23628 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **open-policy-agent** - **opa** version **>= 0.33.1, < 0.37.0**

CVSS3 Score: 5.3 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	LOW	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
format: make groupIterable sort by row by srenatus · Pull Request #3851 · open-policy-agent/opa · GitHub	github.com text/html	MISC github.com/open-policy-agent/opa/pull/3851
format: don't group iterable when one has defaulted location (#4260) · open-policy-agent/opa@932e4ff · GitHub	github.com text/html	MISC github.com/open-policy-agent/opa/commit/932e4ffc37a590ace79e9b75ca4340288c220239
format: make groupIterable sort by row · open-policy-agent/opa@bfd984d · GitHub	github.com text/html	MISC github.com/open-policy-agent/opa/commit/bfd984ddf93ef2c4963a08d4fdadae0bcf1a3717
Formatting generated code can change ordering of array literals · Advisory · open-policy-agent/opa · GitHub	github.com text/html	CONFIRM github.com/open-policy-agent/opa/security/advisories/GHSA-hcw3-j74m-qc58

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openpolicyagent	Open Policy Agent	All	All	All	All

cpe:2.3:a:openpolicyagent:open_policy_agent:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-23628 : OPA is an open source, general-purpose policy engine. Under certain conditions, pretty-printing an… twitter.com/i/web/status/1…	2022-02-09 21:53:02
/r/netcve	CVE-2022-23628	2022-02-09 22:38:52

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report