New issue

[CVE-2026-26477]Unauthenticated Denial of Service via Directory Traversal in DokuWiki 2025-05-14b "Librarian" #94

Open

Hebing123 opened on Jan 9 · edited by Hebing123 Edits Owner

Summary

An unauthenticated Denial of Service (DoS) vulnerability exists in DokuWiki's media upload functionality. Attackers can exploit improper handling of file names containing colon characters (:) to create deeply nested directory structures, exhausting server CPU resources and rendering the system unavailable.

Github: https://github.com/dokuwiki/dokuwiki/releases/tag/release-2025-05-14b

Vulnerability Description

The vulnerability resides in inc/media.php within the media_upload_xhr() function. When uploading files via the media manager, the qqfile parameter is directly used as the file identifier without validating directory depth. Colons in the filename are interpreted as directory separators (e.g., qqfile=123:123.pdf creates 123/123.pdf). An attacker can craft payloads like qqfile=123:123:...:123.pdf (1000+ colons) to force recursive creation of 1000+ nested directories, causing CPU exhaustion due to filesystem operations.

Technical Details

Vulnerable Code

```
// inc/media.php (media_upload_xhr function)
$id = $INPUT->get->str('qqfile');
[$ext, $mime] = mimetype($id);
...
$res = media_save(
```

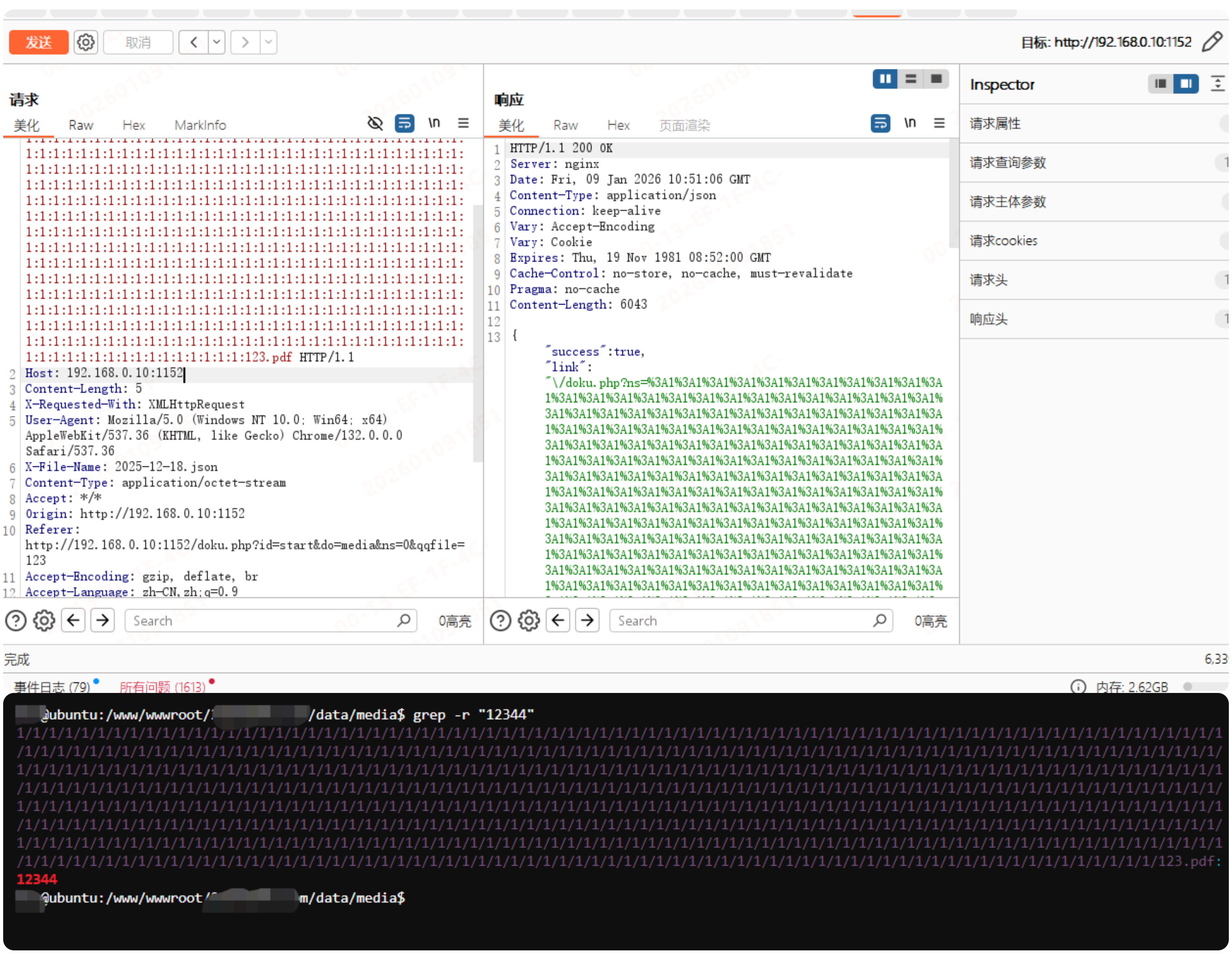
```
    ['name' => $path, 'mime' => $mime, 'ext' => $ext],
    $ns . ':' . $id,
    ($INPUT->get->str('ow') == 'true'),
    $auth,
    'copy'
);
```

Exploitation Steps

Send a POST request to /lib/exe/ajax.php with:

```
POST /lib/exe/ajax.php?
tab_files=files&tab_details=view&do=media&image=e.pdf&ns=&&mediaid=2.pdf&ow=true&call=m
HTTP/1.1
Host: target-ip
Content-Length: 5
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Connection: keep-alive

12344
```



Let's conduct the test using the character blocks in Burpsuite and insert a random number of ":1" into the "qqfile" parameter.

The result is:

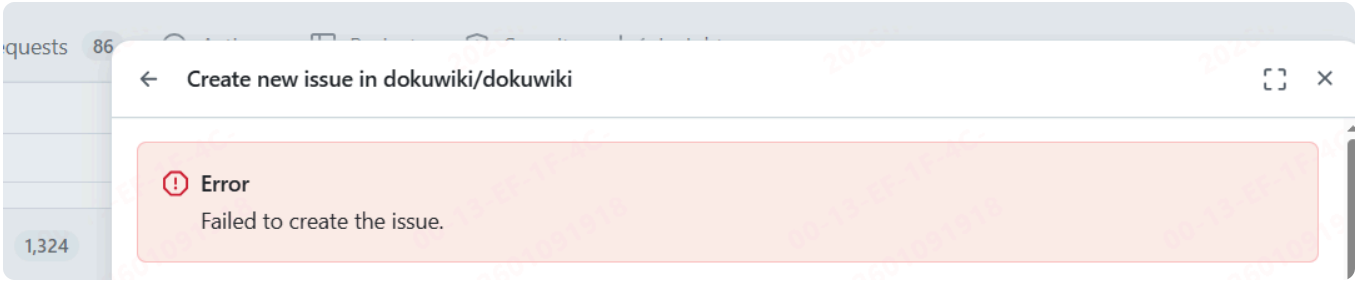
Impact

Service Disruption: CPU exhaustion blocks all legitimate requests.

No Data Exfiltration: The vulnerability is limited to DoS.

INFO

I am not permitted to create questions on DokuWiki. So I created it here to conduct vulnerability alerts.



Hebing123 changed the title ~~Unauthenticated Denial of Service via Directory Traversal in DokuWiki 2025-05-14b "Librarian"~~ [CVE-2026-26477]Unauthenticated Denial of Service via Directory Traversal in DokuWiki 2025-05-14b "Librarian" on Feb 24

splitbrain mentioned this last week

CVE-2026-26477 "Unauthenticated Denial of Service via Directory Traversal"
dokuwiki/dokuwiki#4613

splitbrain last week

Wow! Great job. You fail to create an issue (not sure why BTW) and instead of trying to disclose the issue by mail as described in our SECURITY.md you publish it in your own github repo and request a CVE for it? I only just stumbled by chance about this. WTF?

Further discussion here: dokuwiki/dokuwiki#4613

Hebing123 5 days ago · edited by Hebing123 Edits Owner Author

Response to **@splitbrain** regarding CVE-2026-26477

1. On creating issues
   I didn't "fail" to create an issue—you blocked me. Hard to follow Security.md when the door is locked from the outside.
   Since you think a small bug doesn't matter much, who knows? Maybe I'll have to wait a hundred more years before you reply to my email!
2. On version scope
   Referencing the latest stable version is standard practice for initial vulnerability reports. This establishes a confirmed baseline without implying exclusive impact.
3. On CVE "irresponsibility"
   CVE allocation by MITRE is an identification process, not disclosure. MITRE assigned the CVE because it's valid. You "stumbled across it" because public disclosure works—especially when maintainers block reporters.

4. On the vulnerability
   Resource exhaustion manifests differently across environments—CPU, inode, or memory constraints can all produce DoS conditions. The vulnerability remains valid regardless of specific reproduction thresholds.
   Funny how "not a real bug(bullshit reported again)" gets a fix committed within days. Almost like deep directory nesting is a problem, and resource exhaustion is exploitable—even if your Core Ultra 165H yawns at it.

Conclusion

The report was accurate. The fix proves it. And I'm genuinely surprised you merged the patch despite your tantrum. Credit where it's due. Even if you casually slander me behind my back on some online forum. (https://phpc.social/@dokuwiki/112364095397308541)

Hebing123 pinned this issue 5 days ago

Hebing123 unpinned this issue 5 days ago

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants