6

SQL injection on [redacted] due to tech.cfm

Share:

State	○ Resolved (Closed)
Disclosed	**October 9, 2019 12:27am +0530**
Reported To	**U.S. Dept Of Defense**
Weakness	SQL Injection
Severity	High (7 ~ 8.9)
Participants	
Visibility	Disclosed (Full)

Collapse

SUMMARY BY ALYSSA_HERRERA

The website had an end point like website.mil/xxx/xxx.cfm?sort=grade&type=2. I probed using an apostrophe which resulted in an error. I proceeded to exploit by using a time based query as a proof of concept.

TIMELINE · EXPORT

alyssa_herrera submitted a report to U.S. Dept Of Defense. Jan 29th (2 years ago)

Summary:
The website appears to be vulnerable to SQL injection due to inducing an sql error using a single '

Description:
The following url, https://[redacted]/hro/html/tech.cfm?Sort=Grade&ThisType=2 contains the parameter sort= which is vulnerable to SQLI. We know this due to the error disclosing the SQL query being used.
`SELECT *, tbl_JobInfo.id as TJobID,tbl_JobDocs.id as DocID FROM dbo.tbl_JobInfo left outer join dbo.tbl_JobType on JobTypeID = tbl_JobType.id left outer join tbl_JobDocs on tbl_JobInfo.id = tbl_JobDocs.JobID WHERE JobTypeID = 3 AND JobTypeID > 1 AND Display = 'Y' Order by 'INJECTION' ASC1` We can then demonstrate vulnerability by using time based queries and I opted to instead keep my queries low impact as to not violate the rules.

Impact

High

Step-by-step Reproduction Instructions

https://[redacted]/hro/html/tech.cfm?Sort=SLEEP(25)&ThisType=3
This will cause the page hang to hang momentarily
This won't cause the website to hang, https://[redacted]/hro/html/tech.cfm?Sort=SLEEP()&ThisType=3
Additionally included timing screen shots showing the time between the pages

Product, Version, and Configuration (If applicable)

N/a

Suggested Mitigation/Remediation Actions

Sanitize user input and prepare statements

Impact

An attacker could access the Database and harvest potentially sensitive data from the website or even take over the entire website through using certain SQL commands.

BOT: U.S. Dept Of Defense posted a comment. Jan 29th (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

aboateng updated the severity to Medium. Feb 2nd (2 years ago)

aboateng changed the status to ○ **Triaged**. Feb 2nd (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

aboateng updated the severity from Medium to High. Feb 2nd (2 years ago)

ag3nt-z3 closed the report and changed the status to ○ **Resolved**. Feb 13th (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

alyssa_herrera requested to disclose this report. Feb 13th (2 years ago)

alyssa_herrera posted a comment. Mar 24th (2 years ago)

I'd like this to be disclosed, please.

ag3nt-j7 posted a comment. Mar 24th (2 years ago)

@alyssa_herrera Hi! You are on our list. We are working to standardize the process and expect to be able to close out on all the disclose request soon. Stay tuned!

alyssa_herrera posted a comment. Aug 11th (about 1 year ago)

Alright good to hear

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

disclosure approved

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