5

MSSQL injection via param Customwho in https://[redacted]/News/Transcripts/Search/Sort/ and WAF bypass

Share:

State	○ Resolved (Closed)
Disclosed	**October 11, 2019 12:43am +0530**
Reported To	**U.S. Dept Of Defense**
Weakness	SQL Injection
Severity	High (7 ~ 8.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

ragnar submitted a report to **U.S. Dept Of Defense**. May 12th (5 months ago)

Summary:

MSSQL injection via param `Customwho` in https://[redacted]/News/Transcripts/Search/Sort/

Description:

MSSQL injection via param `Customwho` in https://[redacted]/News/Transcripts/Search/Sort/

There is WAF, but we can make bypass and via global variable `@@LANGID` we can know that the base is used here - MSSQL

Impact

Critical

Step-by-step Reproduction Instructions

Via global variable `@@LANGID` we can find out that here is MSSQL database. [redacted]

https://[redacted]/News/Transcripts/Search/Sort/?Customwho=31002//**|**//@@LANGID

And if use a non-existing global variable, then we get an error. [redacted]

https://[redacted]/News/Transcripts/Search/Sort/?Customwho=31002//**|**//@@nonexisting

Suggested Mitigation/Remediation Actions

Using prepared statement

Impact

We can read and do other manipulations in the database. We can also try to make RCE

BOT: U.S. Dept Of Defense posted a comment. May 12th (5 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

ag3nt-z3 updated the severity to Medium. May 14th (5 months ago)

ag3nt-z3 updated the severity from Medium to High. May 14th (5 months ago)

ag3nt-z3 changed the status to ○ **Triaged**. May 14th (5 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-j1 closed the report and changed the status to ○ **Resolved**. May 17th (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

ragnar requested to disclose this report. Jun 4th (4 months ago)

Hi @deptofdefense @ag3nt-j1,

I would be very grateful if you disclosure this report.

agent-1 agreed to disclose this report. Oct 11th (16 hrs ago)

disclosure approved

This report has been disclosed. Oct 11th (16 hrs ago)