



4

sql injection on /messagecenter/messagingcenter at https://www.██████████/

Share:     State  Resolved (Closed)Disclosed **October 9, 2019 12:17am +0530**Reported To **U.S. Dept Of Defense**

Weakness SQL Injection

Severity  High (7 ~ 8.9)Participants   

Visibility Disclosed (Full)

[Collapse](#)

TIMELINE · EXPORT

**modam3r5** submitted a report to **U.S. Dept Of Defense**.

Jul 15th (about 1 year ago)

Hi ,

i would like to report an issues that lead to SQL injection in search box at <https://www.xn--4zhaaa/messagecenter/messagingcenter> , if you add the character ' that usually used to test if the site have in `sql injection` the site will return with `Incorrect syntax` error that can confirm the site is effected with this bug .

POC

open the following link and enter ' in the box will see this error in response <https://www.xn--4zhaaaaaaa/messagecenter/messagingcenter>

Server Error in '/' Application.

Unclosed quotation mark after the character string ' ORDER BY StartDate2 DESC'.

Incorrect syntax near ' ORDER BY StartDate2 DESC'.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information.

Exception Details: System.Data.SqlClient.SqlException: Unclosed quotation mark after the character string ' ORDER BY

Incorrect syntax near ' ORDER BY StartDate2 DESC'.

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception has been identified.

Stack Trace:

[SqlException (0x80131904): Unclosed quotation mark after the character string ' ORDER BY StartDate2 DESC'.

Incorrect syntax near ' ORDER BY StartDate2 DESC'.]

```
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseIn
System.Data.SqlClient.SqlInternalConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wr
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnecti
System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream,
System.Data.SqlClient.SqlDataReader.TryConsumeMetaData() +61
System.Data.SqlClient.SqlDataReader.get_MetaData() +90
System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptio
System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolea
System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean r
System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean r
System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior, String method) +137
System.Data.SqlClient.SqlCommand.ExecuteDbDataReader(CommandBehavior behavior) +41
System.Data.Common.DbCommand.System.Data.IDbCommand.ExecuteReader(CommandBehavior behavior) +10
System.Data.Common.DbDataAdapter.FillInternal(DataSet dataset, DataTable[] datatables, Int32 startRecord, Int32 m
```

```

System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, Int32 startRecord, Int32 maxRecords, String srcTable, IDbC
System.Data.Common.DbDataAdapter.Fill(DataSet dataSet) +88
GCSS_Army.MessageCenter.MessagingCenter.getMessages(String ssql) in C:\Users\██████████\source\repos\New GCSS-Army\
GCSS_Army.MessageCenter.MessagingCenter.btnSearch_Click(Object sender, EventArgs e) in C:\Users\██████████\source\repos
System.Web.UI.WebControls.Button.OnClick(EventArgs e) +9663950
System.Web.UI.WebControls.Button.RaisePostBackEvent(String eventArgument) +103
System.Web.UI.WebControls.Button.System.Web.UI.IPostBackEventHandler.RaisePostBackEvent(String eventArgument) +16
System.Web.UI.Page.RaisePostBackEvent(IPostBackEventHandler sourceControl, String eventArgument) +13
System.Web.UI.Page.RaisePostBackEvent(NameValueCollection postData) +35
System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint

```

you can use this command `1'; waitfor delay '0:0:2' --` and the error page will return after `2` second

Impact

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.



BOT: [U.S. Dept Of Defense](#) posted a comment.

Jul 15th (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](#) updated the severity to High.

Jul 17th (about 1 year ago)



[ag3nt-z3](#) changed the status to ○ Triaged.

Jul 17th (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](#) posted a comment.

Jul 27th (about 1 year ago)

[@modam3r5](#) it looks like they removed the box. Do you still have a copy of the request in burp that you could test with or send me to make sure it's still not validating the request still?



modam3r5 posted a comment.

Jul 27th (about 1 year ago)

Hi @ag3nt-z3 ,

:\ Unfortunately I deleted all files a few days ago , but i retest the site again and look like the team has remove the effect script/path and i can confirm that look good and fixed now .



ag3nt-z3 closed the report and changed the status to ○ Resolved.

Jul 30th (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



modam3r5 requested to disclose this report.

Jul 5th (3 months ago)

Hi @activities_nyvm @deptofdefense can we change this to public report?!



agent-1 agreed to disclose this report.
disclosure approved

Oct 9th (3 days ago)



This report has been disclosed.

Oct 9th (3 days ago)