38 SQL Injection on www.[redacted] on countID parameter

Share:

State	Resolved (Closed)
Disclosed	October 9, 2019 12:16am +0530
Reported To	U.S. Dept Of Defense
Weakness	SQL Injection
Severity	High (7 ~ 8.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

0_1vitthal submitted a report to U.S. Dept Of Defense. Aug 6th (about 1 year ago)

Description:
Hello Team,
I have came across a sql injection vulnerability on www.[redacted] on countID parameter. I was able to retrieve the banner which is

> Microsoft SQL Server 2008 R2 (SP3) - 10.50.6220.0 (X64&
> Mar 19 2015 12:32:14
> Copyright (c) Microsoft Corporation
> Standard Edition (64-bit) on Windows NT 6.3 <X64> (Build 9600:) (Hypervisor)

after confirming the vulnerability i have stopped testing further.

Vulnerable URL:
https://www.xn--4zhaa/public/saveCount.cfm?countID=4

Steps to Reproduce:

1. python sqlmap.py -u https://www.xn--4zhaaaaaaaaa/public/saveCount.cfm?countID=4 --level=3 --risk=3

POC
[redacted]

Impact

Attacker can take control over the database server.

BOT: U.S. Dept Of Defense posted a comment. Aug 6th (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

0_1vitthal posted a comment. Updated Sep 25th (16 days ago)

According to wiki https://en.wikipedia.org/wiki/Defense_Equal_Opportunity_Management_Institute , The [redacted] may be owned by DoD.
As the Severity of the bug is High I thought reporting to you directly, if it is out of scope of your program Please let me know so i can report the issues to the respective authority.

Thanks,
@0_1vitthal

ag3nt-j1 posted a comment. Aug 10th (about 1 year ago)

@0_1vitthal we're taking a look now, we have a new process here on the backend (not in H1) and we're still getting used to it. Somehow missed your report. The server you found is a DoD asset and is valid.

0_1vitthal posted a comment. Aug 10th (about 1 year ago)

@ag3nt-j1
Thanks for the information.

ag3nt-z3 updated the severity to High. Aug 10th (about 1 year ago)

ag3nt-z3 changed the status to ○ **Triaged**. Aug 10th (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 closed the report and changed the status to ○ **Resolved**. Aug 17th (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

0_1vitthal requested to disclose this report. Aug 20th (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)