

4

IDOR on DoD Website exposes FTP users and passes linked to all accounts!

Share:

State Resolved (Closed)Disclosed **October 4, 2019 8:51pm +0530**Reported To [U.S. Dept Of Defense](#)

Weakness Insecure Direct Object Reference (IDOR)

Severity High (7 ~ 8.9)

Participants

Visibility Disclosed (Full)[Collapse](#)

TIMELINE · EXPORT

cdl submitted a report to [U.S. Dept Of Defense](#).

May 15th (2 years ago)

Description:

[https://\[redacted\]/\[redacted\]](https://[redacted]/[redacted]) is vulnerable to Insecure Direct Object Reference. The application does not validate whether or not who a Push Server belongs to thus allowing an attacker to view the credentials of any FTP / sFTP server linked to any user's account.

Impact

An attacker can view anybody's FTP server information, thus **compromising** the user's FTP servers. This also allows an attacker to **update** or **edit** the Push Server in the [redacted] CMS.

Step-by-step Reproduction Instructions

1. Log into or create an account on [https://\[redacted\]/\[redacted\]](https://[redacted]/[redacted])
2. Now visit [https://\[redacted\]/\[redacted\]/filepush/ftp/303/](https://[redacted]/[redacted]/filepush/ftp/303/)

You will be able to see my ftp server details and you will be able to update or delete it!

An attacker can bruteforce the id to see if the server gives back a valid response. The attacker can then log into the person's FTP servers with the credentials stolen using this vulnerability, giving them full access to private / confidential information!

Example: [https://\[redacted\]/\[redacted\]/filepush/ftp/1/](https://[redacted]/[redacted]/filepush/ftp/1/)

Hostname: [redacted]

Username: [redacted]

Password: [redacted]

Path: /from_pub/cr/[redacted]

[https://\[redacted\]/\[redacted\]/filepush/ftp/<ID>/](https://[redacted]/[redacted]/filepush/ftp/<ID>/)

Suggested Mitigation/Remediation Actions

Check whether or the user's account should have access to the specified Push Server

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

May 15th (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

 [bwluebberhill](#) updated the severity to High.

May 16th (2 years ago)



[bwluebberhill](#) changed the status to ○ **Triaged**.

May 16th (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



[bwluebberhill](#) posted a comment.

May 25th (2 years ago)

Greetings [@cdl](#),

We have been advised that the vulnerability you reported has been resolved. Before we close this report, we would appreciate it if you could confirm that the vulnerability no longer exists.

If we do not receive a response within two weeks, we will send you a second request. If we do not receive a response from you within two weeks of the second notice, we will close this report as resolved.

If you do not believe this vulnerability has been effectively resolved or if you have any questions, please let us know.

Thank you for your time and effort to improve the security of the DoD information network.

Regards,

The VDP Team



[cdl](#) posted a comment.

May 25th (2 years ago)

I can confirm this is fixed! Thanks!



[bwluebberhill](#) closed the report and changed the status to ○ **Resolved**.

May 25th (2 years ago)

Good news!

The vulnerability you reported is considered resolved and this report is now closed. If you have any questions, please let me know.

Thank you for your time and effort to improve the security of the DoD information network.

Regards,

The VDP Team



[cdl](#) requested to disclose this report.

May 25th (2 years ago)

Sweet! Can we disclose this?



cdl posted a comment.

May 28th (2 years ago)

Am I allowed to write about this on my blog if I redact some of the information such as the domain and change other info such as the path?



cdl posted a comment.

Jun 1st (2 years ago)

Hey there, could you check my above requests? I would like permission to do a write up about this vulnerability (I will redact some of the information such as the domain & change other info such as path)



amanion reopened this report.

Jun 1st (2 years ago)



amanion posted a comment.

Jun 1st (2 years ago)

Requesting disclosure, please wait for someone from the Publishing team to comment.



cdl posted a comment.

Jun 1st (2 years ago)

Ok! Thanks @amanion!!



cdl posted a comment.

Jun 6th (2 years ago)

Sorry if I sound impatient, but any updates? This is definitely a fun report that I think deserves to be disclosed ;) Thank you!



cdl posted a comment.

Jun 23rd (2 years ago)

Any updates...?



cdl posted a comment.

Jul 3rd (2 years ago)

Hey there, any updates? It's been a month!!



cdl posted a comment.

Jul 5th (2 years ago)

@amanion Can we get someone from the publishing team to comment? Much appreciated!



cdl posted a comment.

Jul 11th (2 years ago)

Anybody there?



cdl posted a comment.

Jul 13th (2 years ago)

?



cdl posted a comment.

Jul 29th (2 years ago)

Hello, Can we get this resolved please?? This issue is patched already...



jland closed the report and changed the status to Resolved.

Aug 7th (2 years ago)

Hi @cdl -- apologies for reopening here, that was an error on our part. I am re-resolving the ticket so that it can go into the queue for our publications folks.

Thanks!

The VDP Team



cdl posted a comment.

Sep 27th (2 years ago)

Hello? Can we get partial disclosure? Thanks



cdl requested to disclose this report.

Oct 7th (2 years ago)



cdl posted a comment.

Apr 20th (about 1 year ago)

Could we get this partially disclosed? Thanks.

deez_nops posted a comment.

Apr 20th (about 1 year ago)



@cdl Unfortunately, not yet. We are in the final steps to standardize the disclosure process and working through the researchers requests, including your report. Thanks again for your patience.



cdl posted a comment.

Apr 20th (about 1 year ago)

No problem @ag3nt-s21, saw some friend's reports disclosed so was just curious! Thanks for the quick response, I appreciate it!



cdl posted a comment.

Jan 11th (9 months ago)

Hey @ag3nt-s21 / @ag3nt-z3,

Could this be disclosed?

Thanks.



deez_nops posted a comment.

Jan 11th (9 months ago)

@cdl Not yet but, it's in queue to be reviewed.



ag3nt-j1 agreed to disclose this report.

Oct 4th (7 days ago)



This report has been disclosed.

Oct 4th (7 days ago)



U.S. Dept Of Defense has locked this report.

Oct 4th (7 days ago)