

1

Online training material disclosing username and password

Share:     State ☐ Resolved (Closed)Disclosed **October 9, 2019 12:11am +0530**Reported To [U.S. Dept Of Defense](#)

Weakness Insecure Storage of Sensitive Information

Severity  High (7 ~ 8.9)Participants 

Visibility Disclosed (Full)

[Collapse](#)

TIMELINE · EXPORT

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

Aug 14th (2 months ago)

Summary:

A training document is revealing username and password details for what appears to be a DoD training system

Description:

Using the google dork `site:*.mil ext:ppt intext:password`, I was able to find a number of powerpoint documents on .mil websites that include username and passwords.

This document appears to be some old training materials

Slide 39 of [www.██████████.██████████](#) 

See: 

In this instance, the document relates to an online training platform at <https://██████████.██████████/>, so if the credentials are still valid, anyone who reads that presentation could potentially access that system and any data it holds. Training databases often have elements of sensitive data left over from old production databases, so this may expose sensitive information.

Please note that I did not attempt to login using the credentials, as I didn't want to violate any terms of your policy.

If you would like me to attempt to login to test this vulnerability, please let me know.

Step-by-step Reproduction Instructions

Using the google dork `site:*.mil ext:ppt intext:password`, examine any results which appear to include usernames or passwords

See: 

Impact

Attackers may be able to access the contents of either system, which could include sensitive data.

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

Aug 14th (2 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

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

Aug 14th (2 months ago)



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

Aug 14th (2 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**.

Aug 21st (2 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



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

Aug 21st (2 months ago)


Thank you! Can we disclose please?



[agent-1](#) agreed to disclose this report.

Oct 9th (3 days ago)

Disclosure approved

 This report has been disclosed.

Oct 9th (3 days ago)