


13

[REDACTED] Site Exposes [REDACTED] forms

Share:     State ☐ Resolved (Closed)Disclosed **April 6, 2019 1:15am +0530**Reported To [U.S. Dept Of Defense](#)

Weakness Insecure Direct Object Reference (IDOR)

Severity Critical (9 ~ 10)Participants   

Visibility Disclosed (Full)

[Collapse](#)

TIMELINE · EXPORT

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

Aug 15th (about 1 year ago)

Summary

The [REDACTED] site ([https://\[REDACTED\].mil/](https://[REDACTED].mil/)) allows authenticated users to submit [REDACTED] e-forms. Due to a vulnerability in this system, any authenticated user can access the full [REDACTED] e-form of any other user.

Steps to reproduce

1. Intercept an authenticated request on [REDACTED] containing an Authorization header.
2. Replace the url with [REDACTED]. Observe that the id in the url can be incremented/decremented to view recently generated OMPFs.
3. Upon submitting the request, the user's full [REDACTED] form JSON response will be sent.

Impact

Access to [REDACTED] is possible through either a Department of Defense Self-Service logon, CAC card, or [REDACTED] password. Thus, a compromise of a single account on any of these systems would allow for unrestricted access to all [REDACTED] forms.

The [REDACTED] form includes the following

- PII such as SSN, DoB, addresses, etc
- Personal remarks
- Other fields related to security clearances, education, marital status, etc

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

Aug 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



cablej_dds posted a comment.

Updated Apr 6th (6 months ago)

Note that this has been submitted alongside a more critical vulnerability to [REDACTED]. Although that vulnerability was remediated, they have not yet addressed this issue.



ag3nt-z3 updated the severity to Critical.

Aug 16th (about 1 year ago)



ag3nt-z3 changed the status to ○ **Triaged**.

Aug 16th (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-j1 changed the status to ○ **Needs more info**.

Aug 27th (about 1 year ago)

Looks like I get an access denied error when trying to modify the URL. Site is running pretty poorly when trying to access from NIPR. Before I close this out as resolved I was wondering if you can take a second look.



cablej_dds changed the status to ○ **New**.

Aug 28th (about 1 year ago)

Hi @ag3nt-j1,

I can confirm it is no longer possible to view forms via this endpoint.

Thanks,

Jack



ag3nt-j1 changed the status to ○ **Triaged**.

Aug 28th (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-j1 closed the report and changed the status to ○ **Resolved**.

Aug 28th (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



[cablej_dds](#) requested to disclose this report.
Hi,

Apr 4th (6 months ago)

As mentioned in the email, I would like to disclose this report in order to demo at an upcoming event.
Thank you,
Jack



[ag3nt-j1](#) agreed to disclose this report.

Apr 6th (6 months ago)



This report has been disclosed.

Apr 6th (6 months ago)