6

[redacted] Authenticated User Data Disclosure

Share:

State	○ Resolved (Closed)
Disclosed	**October 4, 2019 8:46pm +0530**
Reported To	**U.S. Dept Of Defense**
Weakness	Information Disclosure
Severity	High (7 ~ 8.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

deputy submitted a report to **U.S. Dept Of Defense**. May 21st (5 months ago)

Background

The Air Force's [redacted] application is exposing members' personal information to other users with access to the applocaton. We've identified two specific issues, but there may be other similar problems in the same vein as the ones described here. The underlying problem appears to be that users are not prevented from visiting the web addresses (URLs) that return others' data.
[redacted] Home Page: https://[redacted]/[redacted]
Version Number: 1.85.10

Caveats

1. Users must first be able to login to [redacted] in order to exercise these issues. Members' data is not being exposed to just any user on the web, as far as we know
2. All screenshots containing member data were taken with the consent of the member. Personal information has been redacted and replaced with placeholders (Person #1 and Person #2). Person #1 is the logged in user. Person #2 is another user whose data is being accessed by Person #1, with Person #2's consent.

Issue #1: Exposure of Members' Vulnerable Mover List (VML) Status Information

BLUF: Talent Marketplace exposes members' bid/preference information along with the CC's ranking and comments sent to the Air Force Personnel Center to any logged on user in the VML cycle.
When you visit the "My VML Status" page you are presented by the position preferences you've chosen, the bids you've received, your Losing Commander's comments/ranking, and some other information about your VML cycle. See [redacted]

In order to present you with this information, your browser makes a request in the background for the information it uses to populate the webpage. This request is easily viewable using developer tools present in most modern browsers.

[redacted] shows the raw data sent to your browser in response to the request it sends. You can see all the preferences you put in, information on the bids you've received, and your Losing Commander's ranking and comments for the member. Notice the redacted "personId" labeled "ID #1" at the very top of the screenshot. This is a unique ID tied to Person #1 (you). If you replace this ID with that of Person #2, and make the request again, the server will send you all the same information for Person #2, even though you (not Person #2) are making the request.

Taken to the nth degree, any user could iterate through all "personId" values to gather all bid/preference/CC comments for everyone in a VML cycle, but there's also a way to determine the "personId" of any arbitrary user.

Finding a Member's PersonID

On the "My Profile" page, there's a button you can click to change your military supervisor. When you begin typing someone's name in the dialog box, your browser makes another background request to search the server's database for users with that name. Contained in the response is the user's "personId." This is not necessarily a problem in and of itself, but it can be used to determine the Person ID of the member whose VML Status you wish to see. See [redacted].

Key URLs

Note: You must first log in to the [redacted] application before visiting these URLs

Access Arbitrary Member's VML Cycle Info By Person ID (Replace XXXXXX with Person ID)

https://[redacted]/[redacted]/IndividualReport/GetVmlEligibleBidInfoData?personId=XXXXXX&vmlCycleId=4

Determine Arbitrary Member's Person ID By Name (Replace XXXXXX with Name)

https://[redacted]/[redacted]/SearchPersonUser/FindPerson?SearchTerm=XXXXXX

Issue #2: Exposure of Other Members' Career Brief

BLUF: [redacted] exposes other members' career brief to any logged on user.

When you view the "My Boards" section of [redacted], there's a link that you can visit to see a PDF of your career brief as seen by the Board. The URL for this PDF uses another unique ID (not the same as PersonID from Issue #1) to determine whose career brief you see. If you replace your unique ID with someone else's in the URL, you can see their Career Brief, which contains Privacy Act data. See [redacted].

Finding a Member's "Encrypted ID"

The Career Brief page uses an "Encrypted ID," to identify a member. It is much longer than a "Person ID," making it difficult to just iterate over all possible IDs, but there is a way for you to find the Encrypted ID of a particular user if they have a mentor profile. When you view the members' mentor profile in the "Mentoring Connections" section of [redacted], the URL contains their Encrypted ID. If you copy and paste that ID and replace your ID with theirs in the URL for your career brief, you will see their career brief, which is clearly marked as Privacy Act Data, and should not be visible to any member. See [redacted]

Key URLs

Note: You must first log in to the [redacted] application before visiting this URL

Access Arbitrary Members' Career Brief By Encrypted ID (Replace XXXXXX with Encrypted ID)

https://[redacted]/[redacted]/Dashboard/CareerBrief/PrintOfficerCareerBrief?person=XXXXXX

Suggested Mitigations

We suggest that [redacted] enforce access to user data based on the current logged in user, rather than just the PersonID or Encrypted ID the user presents in the request URL.

It's likely that there are other API endpoints accessible to the user that have similar issues to the two presented above. We also recommend surveying all API endpoints to ensure they are properly validating that the logged in user is only requesting their own information rather than that of any other user.

Impact

Any user logged into USAF [redacted] can see data, including Privacy Act data, of other users through the application. The issue does not expose user data to the open Internet, but it does expose it to other legitimate users who should not be able to see it.

BOT: U.S. Dept Of Defense posted a comment. May 21st (5 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. May 22nd (5 months ago)

deez_nops changed the status to ○ **Triaged**. May 22nd (5 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

deputy posted a comment. Updated May 30th (4 months ago)

VDP Team,
Any update on this? Have the system owners responded to the report at all?

Also, once this issue has been confirmed resolved, is there any restriction on sharing this report with other DoD employees (not publicly)?

Deputy

deez_nops posted a comment. May 30th (4 months ago)

@deputy Nothing to report yet. It has been forwarded to the system owner, however. There is no authorization to disclose until it is mitigated, you request disclosure and it goes through the proper process.

deputy posted a comment. Jun 19th (4 months ago)

Still no word on this? I've heard through the grapevine that the developers have patched the issue, but I'd like for this to be disclosed so I can share my experience and raise awareness of the VDP.

ag3nt-j1 posted a comment. Jun 19th (4 months ago)

@deputy we haven't received anything from the system owner that there was a fix applied to the server, I just took a look at our internal tracker to make sure it didn't come back to us for validation and it hasn't. I'll take a look and validate if the vulnerability was patched or not and try and take it from there.

deez_nops closed the report and changed the status to ○ **Resolved**. Jun 24th (4 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

deputy posted a comment. Jun 26th (4 months ago)

Thank you! I'd like to request disclosure so I can spread the word on the VDP using my experience as an example!

deputy requested to disclose this report. Jun 28th (4 months ago)

As stated above...

deputy posted a comment. Jul 18th (3 months ago)

Any updates on this disclosure request?

ag3nt-j1 posted a comment. Jul 18th (3 months ago)

@deputy working on it. Have several reports I've trying to get redacted and through out internal disclosure process so it tight.

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)