4

Information Disclosure (can access all [redacted]s) within [redacted] view [redacted] Portal

Share:

State	○ Resolved (Closed)
Disclosed	**October 9, 2019 12:28am +0530**
Reported To	U.S. Dept Of Defense
Weakness	Information Disclosure
Severity	High (7 ~ 8.9)
Participants	
Visibility	Disclosed (Full)

Collapse

SUMMARY BY U.S. DEPT OF DEFENSE

An information disclosure vulnerability was discovered on a DoD system.

TIMELINE · EXPORT

archang31 submitted a report to U.S. Dept Of Defense. Jan 23rd (9 months ago)

Summary: Once [redacted] authenticated (I did not mess around to see if I could reproduce without authentication), any user can view any [redacted] simply by changing the offasgid HTTP GET parameter value in the [redacted] view [redacted] portal link.

Description:
I was looking through my previous [redacted]s and noticed I was receiving urls like https://[redacted]/portal/viewrfo.aspx?offasgid=MjAwODAyMTg1Nw== . This url is clearly expecting a HTTP GET parameter offasgid with some base64 encoded value. Decoding this value, you get 2008021857 . The [redacted] in question was my first [redacted] from February 2008. From testing several IDs, I determined the format is {year}{[redacted] #} so 2008, [redacted] # 021857. I simply incremented this value to 2008021858, base64 encoded this value, and browsed to https://[redacted]/portal/viewrfo.aspx?offasgid=MjAwODAyMTg1Ng== . Here, I was able to see [redacted]. I also tested the next value (https://[redacted]/portal/viewrfo.aspx?offasgid=MjAwODAyMTg1NQ==) and got [redacted]. Finally, I opened a new private browser window (so no cookies) and browsed directly to that last link. I had to reauthenticate, but I then was able to directly assess [redacted]. At this point, I stopped interacting with the website to submit this vulnerability.

NOTE: I did not save any record of these [redacted]s outside except the single attached screenshot.
NOTE2: I tried a couple more values during this write-up to better understand the ID. I initially thought the 02 from 2008021858 was the month {year}{month}{id} but its just {year}{id}. I used 2018000001 and ended up with an [redacted] from 20171001 (the very first day of the 2018 fiscal year). I also tested a couple IDs to see how far back the data goes. I used 1999000001 to pull an [redacted] from 19980327. I believe this is the very first [redacted] in the system. I tried 1997000001 as well, and it simply returned a blank [redacted] (i.e. the ID does not exist).

Impact

In a relatively simple and predictable manner (due to the sequential IDs), any user with access to [redacted] can incrementally view every [redacted] issued by [redacted] dating back to 1998. This data includes SSN last 4, EFMP information, branch, and assignment information. From this data, one can extract all sorts of information about the U.S. [redacted] personnel including total [redacted] strength, [redacted] strength by branch, assignment history, strength by base, etc.

Step-by-step Reproduction Instructions

1. Log into [redacted] (https://[redacted].[redacted].[redacted].mil/)
2. Browse to any [redacted] you want to view like https://[redacted]/portal/viewrfo.aspx?offasgid=MjAxOTAxMDg2NQ== if you want to view my most recent [redacted].
3. Modify offasgid value as desired to view any other [redacted] (they seem to be incrementing IDs by year)

Product, Version, and Configuration (If applicable)

Suggested Mitigation/Remediation Actions

First, the offasgid needs to be random and not a predictable value. Secondly, there needs to be some access check based on the provided cookie (user credentials) to ensure that user should be able to access that record.

Impact

In a relatively simple and predictable manner (due to the sequential IDs), any user with access to [redacted] can incrementally view every [redacted] issued by [redacted] dating back to 1998. This data includes SSN last 4, EFMP information, branch, and assignment information. From this data, one can extract all sorts of information about U.S. [redacted] personnel including total [redacted] strength, [redacted] strength by branch, assignment history, strength by base, etc.

BOT: U.S. Dept Of Defense posted a comment. Jan 23rd (9 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

ag3nt-j1 updated the severity to High. Jan 23rd (9 months ago)

ag3nt-j1 changed the status to ○ **Triaged**. Jan 23rd (9 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 changed the status to ○ **Needs more info**. Jan 29th (9 months ago)

Looks like the fix was to properly configure access control to all the documents. When you have a moment can you take a look and verify that the mitigation that was put in place is actually working for you. Side note, I do not think that they are actually going to address the trivial (ie none) sequence of record IDs or the Base64 encoding.

Also, sorry for the form letter. Tied up with about 1 million things going on at the moment...

archang31 changed the status to ○ **New**. Updated Sep 25th (16 days ago)

Awesome - I am impressed at how fast this issue was fixed. I just tested this issue, and it seems fixed. I can access my own [redacted]s, and I get a "You do not have access to this assignment record" when trying to access other [redacted]s. It also gives the same error when you try to access an [redacted] that does not even exist which is great (i.e. I can not differentiate between an [redacted] I simply do not have access too and [redacted]s that do not exist).

No worries about any delays on your side, and I am sure you are super busy. I am just so happy there is a vuln disclosure process to get these fixed - much better than any experience I have had previously trying to get issues fixed.

ag3nt-j1 posted a comment. Jan 29th (8 months ago)

Not a problem, thanks for taking a second look for me. Looked like it was resolved but as you have a record in there I wanted to make sure you couldn't pivot from that point. Usually high and critical findings get pretty fast turnaround. Low level stuff, like low STIG and SRG findings tend to take much longer.

ag3nt-j1 changed the status to ○ **Triaged**. Jan 29th (8 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**. Jan 29th (8 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

archang31 posted a comment. Feb 1st (8 months ago)

Can I have permission to disclose this vulnerability? I would like to share it with some of my peers to remind them of the vuln program and to show how quickly issues get fixed when reported.

ag3nt-j1 posted a comment. Feb 1st (8 months ago)

Damn straight you can and I'd recommend it. Well written reports like yours are good to share with your peers but also other researcher that are just starting out.

ag3nt-j1 posted a comment. Feb 1st (8 months ago)

Did it for you. Expect this to get processed beginning of next week, I'll need to review and redact.

archang31 posted a comment. Feb 7th (8 months ago)

I did not realize agreeing on my end would fully disclose it immediately. The report still contains some names and PII (last 4) that should be redacted.

ag3nt-j1 posted a comment. Feb 7th (8 months ago)

@archang31, I had no idea initiating the disclosure request on my end would give you an option to accept and have the full report published. Report was placed in limited disclosure while we get this straightened out.

archang31 requested to disclose this report. Feb 7th (8 months ago)

@ag3nt-j1 No worries. I think the issue was that I was supposed to request disclosure (i.e. initiate the disclosure request) on my end which then gives you the final disclosure authority. Instead, I just posted a comment because I did not realize that I had other options so you started the process giving me the final disclosure authority.

I apologize for the confusion and believe I started the process correctly on my end now. Let me know if you need anything else.

agent-1 agreed to disclose this report. Oct 9th (3 days ago)

disclosure approved

This report has been disclosed. Oct 9th (3 days ago)