

TIMELINE · EXPORT



thermaltpp submitted a report to U.S. Dept Of Defense.

Oct 25th (12 months ago)

NOTE! Thanks for submitting a report! Please replace *all* the [square] sections below with the pertinent details. Remember, the more detail you provide, the easier it is for us to triage and respond quickly, so be sure to take your time filling out the report!

Summary: [add summary of the vulnerability]

I'm able to take over the admin panel, allowing me to viewing the entire ticket database's PII (DOD ID, email, name by changing the URL and bypassing authentication

Description: [add more details about this vulnerability]

Steps To Reproduce:

1: Go to

?x-app=itsm&x-urlpath=/arsys/shared/login.jsp&x-redir=%2Farsys%2Fforms%2Fedgelb-itsm-ar%2FRKM%253AKnowledgeArticleManager%2FDisplay%2BView%2F%3Feid%3DKBA000000024701%26cacheid%3Ddf8e1567

2: Change URL to

?x-app=itsm&x-urlpath=../../../../../passwd

3)

LFI fails, click login

4) Enjoy full admin panel access

5 (Leak PII)

In the left hand corner, applications -> quick links -> AR system report console Bottom left, click run

Supporting Material/References:

• List any additional material (e.g. screenshots, logs, etc.) Proof of PII:

Proof of admin panel:



I can steal users DOD IDs, pretty much anything I want because I'm the websites admin

Change tickets

Change user info

Change permission

Steal PII



coffeecup (HackerOne staff) posted a comment.

Updated Oct 4th (7 days ago)

@thermaltpp - Excellent report! Please delete the screenshots from Gyazo and upload them here - you can click on this button at the bottom of the page where you write a comment:



tescoramen (HackerOne staff) changed the status to O Triaged.

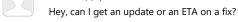
Oct 25th (12 months ago)





thermaltpp posted a comment.

Jan 13th (9 months ago)





coffeecup (HackerOne staff) posted a comment.

Jan 15th (9 months ago)

HI @thermaltpp - We are still working on getting this to the proper remediation team. Thanks for your patience so far, we should have an update soon.



ag3nt-j1 changed the status to O Needs more info.

Nope, still works ;(Attached a PoC Video with steps

Jan 25th (9 months ago)

@thermaltpp can you take a look at your finding and see if you can still reproduce? System owner states that they can't get the PoC to work, I just tried it as well and get back "You do not have sufficient privileges to access the AESD CRM Customer Support Portal." Could be they got a fix in place but didn't document it.



thermaltpp changed the status to O New.

Jan 25th (9 months ago)



ag3nt-j1 posted a comment.

Jan 25th (9 months ago)

Crap, I see now. I wasn't trying to pass my CAC credentials through. Yep, still broken. Reason the system owner doesn't see an issue is that they probably have access to the system.



ag3nt-j1 changed the status to O Triaged.

Jan 25th (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



thermaltpp posted a comment. Would this qualify for a bounty? Jan 25th (9 months ago)



ag3nt-j1 posted a comment.

Jan 25th (9 months ago)

Sorry to say but DoD VDP is not a bounty program. https://hackerone.com/deptofdefense

Any update on a fix? I'd love to do a write-up or a blog post about this if that's allowed.



thermaltpp posted a comment.

Mar 9th (7 months ago)



ag3nt-j1 changed the status to O Needs more info.

Mar 18th (7 months ago)

looks like the system owner has taken care of the access control and admin panel/admin access issue. It now appears that my normal login credentials are passed and I log in as me without any privilege escalation. I have limited view and access into anything now. Take a look when you have a moment and let me know if there is anything else that is an issue.



thermaltpp changed the status to \circ New.

Yep! It's fixed on my end now to.

Mar 18th (7 months ago)



ag3nt-j1 closed the report and changed the status to O Resolved.

Mar 18th (7 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.

Thanks for taking a second look for me on this, looked good from my end I just wanted to make sure. If you want to disclose this report go ahead and request disclosure from the dropdown and we'll work on getting it redacted and published out in H1.

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

Regards,

The VDP Team



thermaltpp requested to disclose this report.

Mar 18th (7 months ago)



thermaltpp posted a comment. Any update on the disclosure? May 3rd (5 months ago)



deez_nops posted a comment.

May 3rd (5 months ago)

@thermaltpp Nothing to report yet but we will keep you posted. Thanks for checking in!



thermaltpp posted a comment.

Jul 18th (3 months ago)

Any update on disclosure?



agent-1 agreed to disclose this report.

Oct 9th (3 days ago)

disclosure approved



This report has been disclosed.

Oct 9th (3 days ago)