22

Trace.axd page leaks sensitive information

Share:

State	Resolved (Closed)
Disclosed	**August 19, 2019 5:51pm +0530**
Reported To	**U.S. Dept Of Defense**
Weakness	Information Exposure Through Debug Information
Severity	Critical (9 ~ 10)
Participants	
Visibility	Disclosed (Full)

Collapse

SUMMARY BY ARINERRON2

See the writeup at https://aaronesau.com/blog/posts/5

TIMELINE · EXPORT

arinerron2 submitted a report to **U.S. Dept Of Defense**. Apr 1st (6 months ago)

Summary

`Trace.axd` leaks sensitive information on [redacted] by allowing signed in users to view previous requests sent to the webserver.

Impact

Information leaked includes (but is not limited to):

- full names
- email addresses
- social security numbers
- dates of birth
- plaintext passwords
- cookies, session tokens, and CSRF tokens
- IP addresses and headers
- application specific information (endpoints, files and directories on the filesystem, software versions,)

Step-by-step Reproduction Instructions

1. Visit https://[redacted]/Gateway/sso.aspx and sign in. Note that any user can create a user (and any privilege level works for this vulnerability as long as a user is signed in), so this should be considered an unauthenticated vulnerability.
2. Visit https://[redacted]/[redacted]/Trace.axd
3. Click on `View Details` for any request that seems interesting. You can find social security numbers by visiting any of the `/candidate_app/dspstatus.aspx` pages and then Ctrl+F'ing for `app_ssn`.

Suggested Mitigation/Remediation Actions

Disable `Trace.axd`. https://docs.microsoft.com/en-us/previous-versions/dotnet/articles/ms972204(v=msdn.10)

Impact

Any attacker can potentially access the following information of current or future Navy personnel:

- full names
- email addresses
- social security numbers
- dates of birth
- plaintext passwords

- cookies, session tokens, and CSRF tokens
- IP addresses and headers
- application specific information (endpoints, files and directories on the filesystem, software versions,)

BOT: U.S. Dept Of Defense posted a comment. Apr 1st (6 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 Critical. Apr 1st (6 months ago)

ag3nt-j1 changed the status to ○ **Triaged**. Apr 1st (6 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**. Apr 11th (6 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

arinerron2 requested to disclose this report. Apr 11th (6 months ago)

Thank you for resolving the issue so quickly! Requesting public disclosure if that's okay.

agent-1 posted a comment. May 6th (5 months ago)

@arinerron2 Thank you for your submission on this critical vulnerability! You have been chosen by our team as a researcher to highlight on our Twitter page @DC3VDP. Do you have a Twitter handle, name, or URL that you would like us to use in our post? Please let us know.

arinerron2 posted a comment. Updated May 7th (5 months ago)

Thank you! And, I have a blog post written and ready for when this report is disclosed.

Twitter (preferred): @arinerron
Name: Aaron E.
URL: https://ww.arinerron.com/

arinerron2 posted a comment. Jul 2nd (3 months ago)

Hi @ag3nt-j1, I'm not sure about the disclosure policy here. Is it possible for these reports to be publicly disclosed? I noticed that the DoD does disclose few, although some, reports.

ag3nt-j1 posted a comment. Jul 2nd (3 months ago)

Sure, you'll have to request disclosure on the report. I'll go in and redact any identifying information that could tie the report to a website and have the attachments deleted before I disclose the report. I have a backlog of disclosure request I need to work through so it might take a little bit of time.

ag3nt-j1 agreed to disclose this report. Aug 19th (2 months ago)

This report has been disclosed. Aug 19th (2 months ago)

arinerron2 posted a comment. Aug 19th (2 months ago)

Thank you @ag3nt-j1! I published the writeup here: https://arinerron.com/blog/posts/5