5 PII leakage-Full SSN on [redacted]

Share:

State	Resolved (Closed)
Disclosed	October 11, 2019 12:44am +0530
Reported To	U.S. Dept Of Defense
Weakness	Insecure Storage of Sensitive Information
Severity	Critical (9 ~ 10)
Participants	
Visibility	Disclosed (Full)

Collapse

SUMMARY BY ALYSSA_HERRERA

This was a simple Google dork search as well as checking other search engines to discover sensitive documents.

TIMELINE · EXPORT

alyssa_herrera submitted a report to U.S. Dept Of Defense. Jul 16th (3 months ago)

Summary:
I discovered a pdf file on [redacted] that outlines various information corresponding to military members. It reveals information on date of birth, where they were born, marriage status, race, children/dependents, etc

Description:
I discovered what looks to be an internal file that outlines sensitive information on various service member and looks to be publicly accessible

Impact

High

Step-by-step Reproduction Instructions

Visit: https://[redacted]/wp-content/uploads/2018/12/[redacted]

Product, Version, and Configuration (If applicable)

N/A

Suggested Mitigation/Remediation Actions

Remove immedietly

Impact

An attacker can gleam highly personal information on military members.

BOT: U.S. Dept Of Defense posted a comment. Jul 16th (3 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

alyssa_herrera posted a comment. Updated Oct 10th (17 hrs ago)

https://[redacted]/wp-content/uploads/2016/12/[redacted]
https://[redacted]/wp-content/uploads/2016/12/[redacted]
https://[redacted]/wp-content/uploads/2016/12/[redacted]

Is another example. Although the SSN is blanked out, everything else there is breach of personal information.

alyssa_herrera changed the report title from **PII leakage on** [redacted] to **PII leakage-Partial SSN on** [redacted]. Updated Oct 10th (17 hrs ago)

alyssa_herrera posted a comment. Updated Oct 10th (17 hrs ago)

I found full SSN, Home address, mother/father name as well on the server. https://[redacted]/wp-content/uploads/2018/12/[redacted]

w0lv3rin3 posted a comment. Jul 16th (3 months ago)

Thanks Alyssa, that file has the full SS#.

alyssa_herrera changed the report title from **PII leakage-Partial SSN on** [redacted] to **PII leakage-Full SSN on** [redacted]. Updated Oct 10th (17 hrs ago)

alyssa_herrera posted a comment. Jul 16th (3 months ago)

I just noticed it actually. I'm still looking for other files on the server

w0lv3rin3 updated the severity to Critical. Jul 16th (3 months ago)

w0lv3rin3 changed the status to ○ **Triaged**. Jul 16th (3 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

alyssa_herrera posted a comment. Updated Oct 10th (17 hrs ago)

https://[redacted]/wp-content/uploads/2016/12/[redacted]
This has a social security on it

alyssa_herrera posted a comment. Updated Oct 10th (17 hrs ago)

Oh quick question. Is there any severity to having credentials to a test instance ?
https://[redacted]/wp-content/uploads/2016/12/[redacted]
lists out credentials and locations to use them in.

alyssa_herrera posted a comment. Updated Oct 10th (17 hrs ago)

https://[redacted]/wp-content/uploads/2019/04/[redacted] this also has PII. There's a screen capture on the 13th slide which you can faintly make out the last 4 digit's of an SSN even if the rest are redacted.

alyssa_herrera posted a comment. Updated Oct 10th (17 hrs ago)

https://[redacted]/wp-content/uploads/2018/12/[redacted]

This also looks to be SSN as well.

I'm going to keep it all in this report instead of filing new ones unless other wise told by the way

alyssa_herrera posted a comment. Updated Oct 10th (17 hrs ago)

https://[redacted]/wp-content/uploads/2018/12/[redacted]

At this rate, the entire server will need to be take down and looked through /scrubbed of documents. I'll keep digging to see what else I can uncover on the server. I noticed a lot of stuffed that is marked with HR docs on it, tended to contain legitimate PII

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

Thanks for digging around on the server. At this point I don't think you need to keep going, we've already tagged the report as critical and I will be reaching out internally to try and get more traction. I've made requests to shut down sites before but at the end of the day it's up to the digression of the system and data owner.

w0lv3rin3 closed the report and changed the status to ○ **Resolved**. Jul 19th (3 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

alyssa_herrera requested to disclose this report. Jul 19th (3 months ago)

agent-1 agreed to disclose this report. Oct 11th (16 hrs ago)

disclosure approved

This report has been disclosed. Oct 11th (16 hrs ago)