12

PII leakage due to caching of Order/Contract ID's on [redacted]

Share:

State	Resolved (Closed)
Disclosed	October 9, 2019 12:18am +0530
Reported To	U.S. Dept Of Defense
Weakness	Information Disclosure
Severity	High (7 ~ 8.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

alyssa_herrera submitted a report to U.S. Dept Of Defense. Jun 30th (about 1 year ago)

Summary:

I was able to discover contract numbers which leak out user names/emails/phone numbers nd other sensitive information. I took the time to assure that these contract id's wouldn't/shouldn't be easy guessable or known.

Description:

I discovered through google search query that I was able to access several Order/contract id's that revealed a trove of sensitive data that shouldn't of been easily accessible or cached by google search results.

Impact

High

Step-by-step Reproduction Instructions

https://[redacted]/CMT_View/CMT_View_List.cfm?StartRow=31&OrderBy=Email&OrderByCol=4&Sort=DESC&SearchType=CONTRACT&ContractNumber=[redacted]&Cage=

https://[redacted]/CMT_View/CMT_View_List.cfm?OrderBy=FormatedRoleCode&OrderByCol=2&StartRow=1&Sort=ASC&SearchType=CONTRACT&ContractNumber=[redacted]&Cage=

[redacted], [redacted] D. ACO 1102 [redacted]@[redacted]
[redacted], [redacted] J. CA 1102 [redacted]@[redacted]
[redacted], [redacted] M. DRPM 0801 [redacted]@[redacted]
[redacted], [redacted] R. IS 1150 [redacted]@[redacted]
[redacted], [redacted] R. PA 1103 [redacted]@[redacted]
[redacted], [redacted] S. PT 1106 [redacted]@[redacted]
[redacted], [redacted] E. QAR 1910 [redacted]@[redacted]
[redacted], [redacted] M. SUP 0344 [redacted]@[redacted]
[redacted], [redacted] R. SUP 1150 [redacted]@[redacted]
[redacted], [redacted] D. SUP 1150 [redacted]@[redacted]

Additionally verified that these aren't test data entries by googling one of the emails and resulting found the owner's linkedin account.

Product, Version, and Configuration (If applicable)

N/A

Suggested Mitigation/Remediation Actions

Impact

An attacker can gather high priority PII.

BOT: U.S. Dept Of Defense posted a comment. Jun 30th (about 1 year 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. Jun 30th (about 1 year ago)

I found several instances of this and estimate around 155 emails/names/phone numbers along with positions were found.

ag3nt-j1 updated the severity to High. Jul 2nd (about 1 year ago)

ag3nt-j1 changed the status to ○ **Triaged**. Jul 2nd (about 1 year 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**. Jul 6th (about 1 year 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 9th (about 1 year ago)

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

disclosure approved

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