19

Access to all [redacted] files, including CAC authentication bypass

Share:

State	Resolved (Closed)
Disclosed	April 8, 2019 10:34pm +0530
Reported To	U.S. Dept Of Defense
Weakness	Insecure Direct Object Reference (IDOR)
Severity	Critical (9 ~ 10)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

cablej_dds submitted a report to U.S. Dept Of Defense. Oct 26th (12 months ago)

Summary:

Due to an Insecure Direct Object Reference (IDOR) in adding recipients to a shared package on [redacted], an unauthenticated attacker can access all files uploaded to [redacted]. As described on [redacted] website, this includes documents with classifications up to FOUO, including PII / PHI Privacy Act data, and documents classified `FOUO//CLOSE HOLD`, `FOUO//SENSITIVE`, and `FOUO//LIMITED DISTRIBUTION DOCUMENT`.

Additionally, [redacted] enforces CAC pickup requirements to require users to first authorize via CAC. This too, can be bypassed, allowing an attacker to download any file sent over [redacted].

Note that in addition to this vulnerability, other IDORs exist in sensitive areas, such as confirming email addresses, allowing an attacker to pretend to send documents from any email address.

Impact

Based on analysis of file ids, over 2000 documents are uploaded per hour to [redacted]. When combined with a [redacted], this exposes over 500,000 recent documents and new documents that are sent every hour. Additionally, as metadata for historical documents is not purged, this also includes details such as sender names/emails, file descriptions, and share dates for over 15 million past documents.

Step-by-step Reproduction Instructions

1. Visit[redacted]/Default.aspx and proceed to send a file to yourself.
2. Click through the verification email and verify the file.
3. Log in to the Package Status page at[redacted]/StatusLogIn.aspx?PackageID=x using the provided password.
4. Intercept the request to add a new recipient via the recipients list, entering your email address as the email to add. This is a `POST` request to `POST /[redacted]/Status.aspx?ID=x`.
5. Modify the `ID` parameter to any other number, e.g. decrement the number by 1.
6. Observe that the package will be sent to your email, which can then be downloaded using the provided password.
7. Repeat with any numeric ID to download hundreds of thousands of files.

To bypass CAC authentication:

A user can elect to require CAC authentication when downloading a file. This can be bypassed via the normal file download flow.

1. Visit[redacted]/[redacted]?id=15745307 (the initial file ID here does not matter).
2. Enter the password emailed for the file that requires CAC authentication.
3. Intercept the request to submit the form. Replace the `id` parameter in the url with the id of the file with CAC authentication.
4. Observe that the file's information will be displayed and can be downloaded.

Suggested Mitigation/Remediation Actions

- Ensure that a user can only modify their own packages

- Ensure that a file cannot be downloaded without CAC authentication
- Ensure that a user can only verify their own packages.

Impact

.

BOT: U.S. Dept Of Defense posted a comment. Oct 26th (12 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

deez_nops changed the status to ○ **Needs more info**. Oct 26th (12 months ago)

Greetings,
Greetings,

To validate your report, We require additional information.

Can you please answer the following questions?

Please provide screen shots of your process, as I was unable to replicate your walkthrough results.

I will continue processing your report on receipt of your response. You will receive another status update upon completion of this review. If I have any other questions in the interim, I will be back in touch.

If we do not receive a response within two weeks, we will send you a second request for this information. If we do not receive a response from you within two weeks of the second notice, we will have to close this report without action.

If you have any questions, please let me know.

Thanks again for supporting the DoD Vulnerability Disclosure Program.

Regards,

Thanks again for supporting the DoD Vulnerability Disclosure Program.

Regards,

The VDP Team

cablej_dds changed the status to ○ **New**. Updated Apr 8th (6 months ago)

Hi @ag3nt-s21,

Please see as follows:

1. Create a [redacted] package. For convenience, you may log into one I've created at [redacted]/StatusLogIn.aspx?PackageID=15741848 with password [redacted]
2. Scroll to the bottom. Add your own email under the `Add New Recipient` section and intercept the request to `POST /[redacted]/Status.aspx?ID=15741848` in Burp Suite to submit the form:

   {F366694}

{F366695}

3. Modify the `ID` parameter in the url of the request to `15743188`, a different package that I created for testing purposes.
4. Observe that if the email address has not already been invited, you will see the following in the response:

   {F366697}

5. The package will be shared with your email address, which can then be downloaded as normal.

ag3nt-j1 updated the severity to Critical. Oct 30th (12 months ago)

ag3nt-j1 changed the status to ○ **Triaged**. Oct 30th (12 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**. Updated Apr 8th (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.

Closing as resolved as [redacted]

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

Regards,

The VDP Team

cablej_dds requested to disclose this report. Apr 4th (6 months ago)

Hi,

As mentioned in the email, I would like to disclose this report in order to demo at an upcoming event.

Thank you,
Jack

ag3nt-j1 agreed to disclose this report. Apr 8th (6 months ago)

This report has been disclosed. Apr 8th (6 months ago)