



[Critical] Possibility to takeover any user account #2 without interaction on the https://[REDACTED]

Share:     


State Resolved (Closed)

Disclosed **October 4, 2019 8:46pm +0530**

Reported To **U.S. Dept Of Defense**

Weakness Privilege Escalation

Severity Critical (9 ~ 10)

Participants  

Visibility Disclosed (Full)

[Collapse](#)

TIMELINE · EXPORT



sp1d3rs submitted a report to **U.S. Dept Of Defense**.

Apr 21st (6 months ago)

Description

Hello. This time I discovered a way to takeover any user's account via unsafe password reset. This time it's much easier than #1 way in the [#543678](#) report. When users requests the password reset, the next link is come to the email:

```
https://[REDACTED]/resetpassword.aspx?ru=[user_id]&op=[token]
```

The [user_id] is numeric, always same for same email, and incremental for every new user. The [token] parameter is random and used to protect the link from hijacking. But, I discovered that Reset password endpoint accepts empty token!

So all the attacker needs, it's to initiate password reset for the victim's email, and request the

```
https://[REDACTED]/resetpassword.aspx?ru=[user_id]&op=
```

Since [user_id] is numeric and static for same account, it can be easily guessed by the attacker.

POC

- 1) Go to the [https://\[REDACTED\]/ForgotPassword.aspx](#)
- 2) Initiate reset password for the [REDACTED] (it's my test account)
- 3) Use this link:

```
https://[REDACTED]/resetpassword.aspx?ru=7655&op=
```

where 7655 - it's my user numeric ID (as we know, it's incremental, and be easily guessed for other accounts).

- 4) Set the new password and confirm it. You can set something as `11111111aA!!!!` to pass the password requirements.
- 5) You will be logged into my organization as admin.

Suggested fix

Fix the `op` token validation - it should be checked properly.

Impact

Severity: Critical

Immediate account Individual/Corporate account takeover via password reset. Attacker needs to know only email.



BOT: [U.S. Dept Of Defense](#) posted a comment.
Greetings from the Department of Defense (DoD),

Apr 21st (6 months ago)

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 27th (6 months ago)



[ag3nt-j1](#) changed the status to Triaged.
Greetings,

Apr 27th (6 months ago)

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.
Good news!

May 14th (5 months ago)

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

— [sp1d3rs](#) requested to disclose this report.

Jul 11th (3 months ago)

— [ag3nt-j1](#) agreed to disclose this report.

Oct 4th (7 days ago)

— This report has been disclosed.

Oct 4th (7 days ago)

— [U.S. Dept Of Defense](#) has locked this report.

Oct 4th (7 days ago)

