17 [REMOTE] Full Account Takeover At https://[redacted]/CAS/

Share:

State	Resolved (Closed)
Disclosed	October 4, 2019 8:53pm +0530
Reported To	U.S. Dept Of Defense
Weakness	Reliance on Cookies without Validation and Integrity Checking in a Security Decision
Severity	High (7 ~ 8.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

karimrahal submitted a report to U.S. Dept Of Defense. Mar 24th (3 years ago)

Summary:
A session cookie **PROD_CAS_SESSION** takes a User ID as an input, hence an attacker is able to insert his victim's User ID and takeover his victim's account. (P.S The User ID is only 6 numbers long).

Impact

An attacker is able to insert his victim's User ID into the cookie **PROD_CAS_SESSION** and takeover his victim's account.

Step-by-step Reproduction Instructions

1. Go to https://[redacted]/MOS/ (This is one of many websites you can do this from)
2. Add a cookie with the domain [redacted], the name **PROD_CAS_SESSION*, and the value should be ur victim's User ID (example: **195141**).
3. Refresh the page
4. Done, you will be logged into your victim's account.

To Get User's Info

1. At https://[redacted]/MOS/, you will notice a dropdown on the right top corner with **Welcome (Your Victim's Name)**, click the dropdown and click **My Profile**
2. Done, you will be able to see your victim's user info.

Suggested Mitigation/Remediation Actions

Add a more secure session value.

BOT: U.S. Dept Of Defense posted a comment. Mar 24th (3 years 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

styn changed the status to ○ **Triaged**. Apr 3rd (3 years 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

styn updated the severity to Critical. Apr 3rd (3 years ago)

dc34 updated the severity from Critical to High. Apr 4th (3 years ago)

dc34 posted a comment. Apr 4th (3 years ago)

Upon assessing the impact of the vulnerability to their overall mission, the System owners have downgraded this to a high risk and we are adjusting the severity accordingly

karimrahal posted a comment. May 13th (2 years ago)

Any update?

bwluebberthill posted a comment. Jun 30th (2 years ago)

Greetings @karimrahal,

We have been advised that the vulnerability you reported has been resolved. Before we close this report, we would appreciate it if you could confirm that the vulnerability no longer exists.

If we do not receive a response within two weeks, we will send you a second request. If we do not receive a response from you within two weeks of the second notice, we will close this report as resolved.

If you do not believe this vulnerability has been effectively resolved or if you have any questions, please let us know.

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

Regards,

The VDP Team

karimrahal posted a comment. Jun 30th (2 years ago)

Hello!

I can happily confirm that this vulnerability has been successfully patched.
A stronger cryptography is now being used to generate the user id.

Thank You,
Karim Rahal

bwluebberthill closed the report and changed the status to ○ **Resolved**. Jun 30th (2 years ago)

Good news!

The vulnerability you reported is considered resolved and this report is now closed. If you have any questions, please let me know.

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

Regards,

The VDP Team

karimrahal requested to disclose this report. Jun 30th (2 years ago)
I would love if this could be at-least partially disclosed.

karimrahal posted a comment. Aug 16th (2 years ago)
Can this be publicly / partially disclosed on h1 please?

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)