6 Examples directory is PUBLIC on https://[redacted]mil, leading to multiple vulns

Share:

State	Resolved (Closed)
Disclosed	October 11, 2019 12:41am +0530
Reported To	U.S. Dept Of Defense
Weakness	Improper Access Control - Generic
Severity	Critical (9 ~ 10)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

mason357 submitted a report to U.S. Dept Of Defense. Aug 16th (2 months ago)

Description:
Hello,

In an effort to consolidate reporting. I have located 4 issues with having the Examples Directory open(my require just 1 solution to mitigate) The following URLs that show concern are the following:

1. https://[redacted]mil/examples/servlets/servlet/SessionExample <--Will lead to Session Manipulation and potential Account Takeover
2. https://[redacted]mil/examples/servlets/servlet/RequestHeaderExample <---Internal IP disclosure
3. https://[redacted]mil/examples/servlets/ <---Source Code Disclosure and an "Execute" option(did not press Execute button so I am not sure the impact of it.
4. https://[redacted]mil/examples/servlets/servlet/CookieExample <----Insecure Cookie Handling

Step-by-step Reproduction Instructions

1. Please visit the above links 2. 3.

Suggested Mitigation/Remediation Actions

Disable public access to the examples directory as soon as possible!

Impact

Ordered by Highest Impact:

1. https://[redacted]mil/examples/servlets/servlet/SessionExample <--Will lead to Session Manipulation and potential Account Takeover. Because the session is global this servlet poses a big security risk as an attacker can potentially become an administrator by manipulating its session.
2. https://[redacted]mil/examples/servlets/servlet/CookieExample <----Insecure Cookie Handling
3. https://[redacted]mil/examples/servlets/ <---Source Code Disclosure and an "Execute" option
4. https://[redacted]mil/examples/servlets/servlet/RequestHeaderExample <---Internal IP disclosure

deez_nops updated the severity to Critical. Aug 16th (2 months ago)

deez_nops changed the status to Triaged. Aug 16th (2 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

mason357 posted a comment. Aug 27th (2 months ago)
Hello,

Following up

deez_nops posted a comment. Aug 27th (2 months ago)
@mason357 Nothing to report yet.

mason357 posted a comment. Aug 27th (2 months ago)
Thanks, This looks like it was remidiated. I cannot get into any of the files.

mason357 posted a comment. Aug 27th (about 1 month ago)
Following up. I cannot replicate the bug. What are the next steps?

mason357 posted a comment. Aug 29th (about 1 month ago)
Following up, Bug has been fixed? Will this be changed to resolved??

deez_nops closed the report and changed the status to ○ **Resolved**. Aug 30th (about 1 month 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

mason357 posted a comment. Aug 30th (about 1 month ago)
Thank you!!

mason357 requested to disclose this report. Oct 9th (2 days ago)
I'd love to disclose this, I know itll take 84 years but I would like to start the process.

ag3nt-j1 posted a comment. Oct 10th (17 hrs ago)
I think it'll happen a little quicker than 84 years lol.

mason357 posted a comment. Oct 10th (17 hrs ago)
LOL, I know you guys are busy as all hell so I get it :D

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

disclosure approved.

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

mason357 posted a comment. Oct 11th (16 hrs ago)

Thank you my friend, Have a great day :D