

darklotuskdb / CISCO-CVE-2020-3452-Scanner-Exploiter

Public

Notifications

Fork 30

Star 98

<> Code

Issues 1

Pull requests

Actions

Projects

Security

Insights

main

Go to file

<> Code

darklotuskdb

Add files via upload

89cedbd · 3 years ago

14 Commits

LICENSE	Initial commit	4 years ago
README.md	Update README.md	4 years ago
SnE-CVE-2020-3452.sh	Update SnE-CVE-2020-3452.sh	4 years ago
update.sh	Add files via upload	3 years ago

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

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

### 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

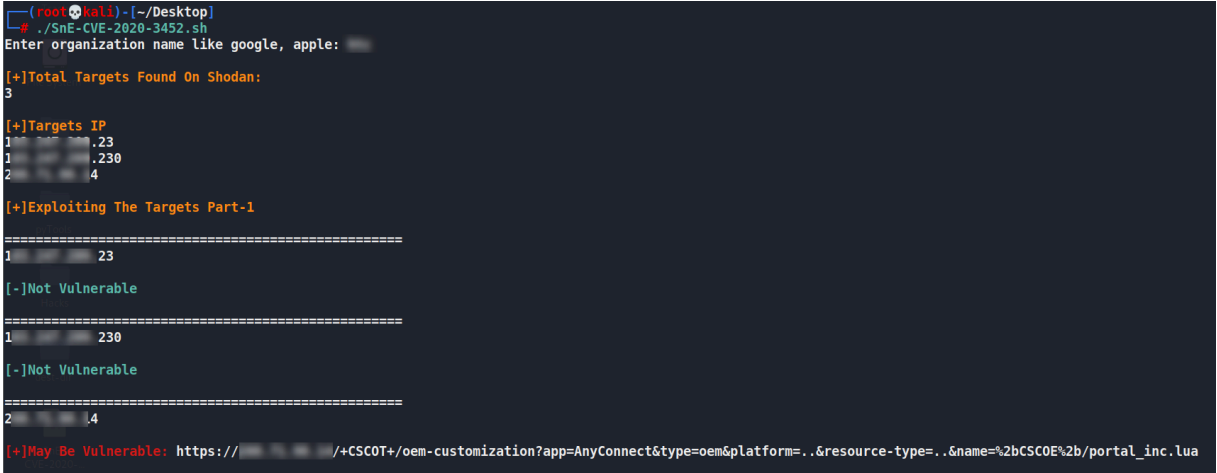
Shell 100.0%

Page 1 of 2

- git clone https://github.com/darklotuskdb/CISCO-CVE-2020-3452-Scanner-Exploiter
  - cd CISCO-CVE-2020-3452-Scanner-Exploiter/
  - chmod +x SnE-CVE-2020-3452.sh
  - ./SnE-CVE-2020-3452.sh



### Screenshot



### Reference

- <https://twitter.com/aboul3la/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](#)

