Romania
University POLITEHNICA of Bucharest
Faculty of Automatic Control and Computers
Advanced Cybersecurity

CVE-2021-41773

Student
George-Andrei IOSIF

Bucharest
2022

Introduction

Introduction

- Apache HTTP Server, a free and open source web server

Introduction

- Apache HTTP Server, a free and open source web server
- Path traversal found in October 2021

Introduction

- Apache HTTP Server, a free and open source web server
- Path traversal found in October 2021
- Escalated in remote code execution if CGI is enabled

Vulnerability Analysis

Vulnerability Analysis

- Weak path normalization in 2.4.49

Vulnerability Analysis

- Weak path normalization in 2.4.49
- `Directory` set to `Require all granted`

Vulnerability Analysis

- Weak path normalization in 2.4.49
- `Directory` set to `Require all granted`
- `/cgi-bin/../../../../<path_to_file>` for information disclosure

Vulnerability Analysis

- Weak path normalization in 2.4.49
- `Directory` set to `Require all granted`
- `/cgi-bin/../../../../<path_to_file>` for information disclosure
- `/cgi-bin/../../../../bin/bash`, CGI and `POST`-ed commands for remote code execution

Impact

Impact

- Arbitrary file read

Impact

- Arbitrary file read
- (Limited) Code execution

Impact

- Arbitrary file read
- (Limited) Code execution
- `Administrator` or `root` capabilities when chained with a local privilege escalation

Mitigations

Mitigations

- Upgrade to 2.4.51

Mitigations

- Upgrade to 2.4.51
- IP blacklists

Mitigations

- Upgrade to 2.4.51
- IP blacklists
- IPS rules

Exploitation in the Wild

Exploitation in the Wild

- 0-day vulnerability before releasing the advisory

Exploitation in the Wild

- 0-day vulnerability before releasing the advisory
- 100.000+ vulnerable web servers via Shodan

Exploitation in the Wild

- 0-day vulnerability before releasing the advisory
- 100.000+ vulnerable web servers via Shodan
- Posts on cybercrime forums

Exploitation in the Wild

- 0-day vulnerability before releasing the advisory
- 100.000+ vulnerable web servers via Shodan
- Posts on cybercrime forums
- Detections in Trend Micro's honeypots

Exploitation in the Wild

- 0-day vulnerability before releasing the advisory
- 100.000+ vulnerable web servers via Shodan
- Posts on cybercrime forums
- Detections in Trend Micro's honeypots
- Usage in RATs and miners

Conclusions

Conclusions

- O-day, but discovered in time

Conclusions

- O-day, but discovered in time
- Patch as a straightforward mitigation

Conclusions

- O-day, but discovered in time
- Patch as a straightforward mitigation
- Continuous exploitation in the wild

Conclusions

- 0-day, but discovered in time
- Patch as a straightforward mitigation
- Continuous exploitation in the wild
- `@iosifache` on GitHub for these LaTeX projects (based on reusable templates) and demo