



# CYOPS TEAM

Cynet's 24/7 MDR with the latest security updates and reports

## FortiOS - Path Traversal vulnerability exploited

**Bank Security** @Bank\_Security

After a nslookup on all IPs, I found that among the victims there are some Banks, many .gov domains and thousands of companies around the world.

**Bank Security** @Bank\_Security · Nov 19

The Threat Actor "pumpedkicks" shared a list of 49,577 IPs vulnerable to Fortinet SSL VPN CVE-2018-13379.

The Actor also claims to have the clear text credentials associated with these IPs.

[Show this thread](#)

Fortinet SSL VPN - 49,577  
by pumpedkicks · Yesterday at 10:58 PM

**pumpedkicks**

I have prepared a list of all targets  
It is a vulnerability of reading log files  
there are 49,577 vulnerable targets  
the order is, ip\_address,username

Access

VIP User

my e-mail for contact

E-mail: @protonmail.com  
Jobber: @mmpa.jp

Denote BTC: 1C4E2Fj6XX761yyNkLwBHz2u0jYv50

Profs: 25  
Threads: 18  
Joined: Nov 2020  
Reputation: 0

A "Path Traversal" vulnerability allows malicious actors to access resources outside a web-server's root folder. Such a vulnerability ("CVE-2018-13379") was previously discovered at FortiOS and patched by Fortinet and was seen used by state backed hackers, when combined with other Windows OS vulnerabilities to [disrupt the support systems of the US government elections \(BleepingComputers.com\)](#).

Unfortunately the vulnerability remains unattended and unpatched by many users. This concern has risen as a new threat actor published a 6.7 GB list including credentials and IP addresses of vulnerable, internet exposed FortiOS Servers. In a tweet [shared by a threat intelligence analyst "Bank Security"](#) the list of credentials were first discovered and then [checked for validity and confirmed by "Bank Security"](#) to be related to Banks, Government domains and other high profile FortiOS users around the world.

We recommend you [Read more about the vulnerability at FortiGaurds Labs](#), where you'll find information about upgrading FortiOS, enabling 2FA for new connections which will help prevent exploitation of the vulnerability.