Analysis of Threat Actor Data Posting

fortinet.com/blog/psirt-blogs/analysis-of-threat-actor-data-posting

January 16, 2025

Affected Platforms: FortiOS 7.0.0 – 7.0.6 and 7.2.0 – 7.2.1
Impacted Users: Various
Impact: Configuration and VPN Password Exposure
Severity Level: High

Executive Summary

Fortinet is aware of a posting by a threat actor which claims to offer compromised configuration and VPN credentials from FortiGate devices. Based on our analysis, the data involved is a resharing of data from previous incidents from dates prior to November 2022 and is not related to any recent incident or advisory. The following provides factual information to help our customers better understand the situation and make informed decisions.

Threat Actor Posting

Fortinet discovered the posting on a forum via the FortiRecon Dark Web Activity Monitoring service. This group, newly created in January 2025, published files that purportedly contain stolen FortiGate data, categorized by country names including:

- IPs
- Passwords
- Configurations

Based on our analysis, the threat actor's claim is misleading.

Analysis of the data

The stolen data is arranged in folders with the IP address and a port on the firewall, in the format 10.20.30.41_xxx where xxx is most commonly 443 or 10443 which suggests this is meant to represent be the SSL-VPN port.

The folders contain two files:

config.conf - The FortiGate configuration backup
vpn-password.txt - Password file containing credentials from the SSL-VPN

config.conf

After analyzing the firmware versions in the exposed configurations, it was immediately clear that the exposed data originates from an older vulnerability, as the list does not include any configurations for FortiOS 7.6 or 7.4, nor any recent configurations for 7.2 and 7.0.

Another indicator was the presence of two other IoCs commonly found in an older published vulnerability.

- Configuration obtained by user Local_Process_Access
- Malicious Admin: fortigate-tech-support

Given both points, it is highly likely that this data was obtained via the previously communicated and resolved vulnerability FG-IR-22-377 / CVE-2022-40684. In addition to the published advisory, we also published further insights and detail in a blog post from October 2022 entitled, "Update Regarding CVE-2022-40684." Data corroborating the findings includes that the threat actor-shared configs are from 7.2.1 and 7.0.6 (which were the last vulnerable versions as noted in our 2022 advisory).

vpn-password.txt

Similar to the configurations, the data in password .txt immediately appeared familiar as it was similar in content and matched data disclosed in a previously resolved FG-IR-18-384 / CVE-2018-13379 vulnerability.

The difference being that the filenames and headers of the files were different. We found a Python file that explains this as this was used to change the filenames and insert the moniker of the Threat Actor into all of the password files.

Filename: 1.py
This was widely communicated at the time in the published PSIRT Advisory, and in a 2019 blog and subsequent blog in 2020.

Conclusion

The threat actor has leaked data obtained in dated campaigns that has been aggregated to appear like a new disclosure. Our analysis of the devices in question show that the majority have long since upgraded to newer versions. If your organization has consistently adhered to routine best practices in regularly refreshing security credentials and taken the recommended actions in the preceding years, the risk of the organization's current config or credential detail in the threat actor's disclosure is small. We continue to strongly recommend that organizations take the recommended actions, if they have not already, to improve their security posture.

We can also confirm that devices purchased since December 2022 or devices which have only run FortiOS 7.2.2 or above are not impacted by the information disclosed by this threat actor.

If you were running an impacted version (7.0.6 and lower or 7.2.1 and lower) prior to November 2022 and did not already take the actions recommended in the advisory, we strongly recommend reviewing the recommended actions to improve your security posture.

Whilst this data is several years old and the IP addresses have been observed to no longer be relevant in many cases, we will be reaching out to any customers, where identified, to recommend to review configurations.

If you are a Fortinet customer and have reviewed this detail and still have questions, please reach out to cs@fortinet.com.

Recommended actions

For our customers, your risk of being impacted by the information disclosed is low if:

- Your device was purchased in December 2022 or after

- Your organization has consistently adhered to routine best practices in regularly refreshing security credentials and taken the recommended actions in past Fortinet PSIRT Advisories

Fortinet recommends that customers:

- Upgrade to the latest patch release for your release train.
- Validate the FortiGate configuration to ensure that no unauthorized changes have been implemented by a malicious third party.
- Look for the known IoCs document in the referenced Incidents (FG-IR-22-377 / FG-IR-18-384).
- Follow best practice recommendations for configuration.