Advisory
28 October 2024
TLP:CLEAR

Critical Vulnerability affecting Fortinet FortiGate Devices (CVE-2024-47575)

This advisory is relevant to Samoan organisations who are running or administering Fortinet FortiGate infrastructure. Relevant organisations are encouraged to apply available mitigations immediately.

What's Happened?

SamCERT has been made aware of a recently disclosed vulnerability within Fortinet FortiGate devices with management interfaces exposed to the internet. The vulnerability may enable actors to bypass authentication and execute commands in these same FortiGate devices. Further analysis indicates several Fortinet devices located in Samoa have exposed management interfaces available on the internet.

How do I stay secure?

- SamCERT strongly advises organisations administering Fortinet and FortiGate infrastructure to implement controls that prevent these management portals from being accessible to the public internet as soon as possible.
- SamCERT also strongly recommends that Samoan organisations managing FortiNet and FortiGate devices conduct a detailed review of the Fortinet logs to assess any instances of historical or current compromise. SamCERT can assist with this analysis if required.
- Organisations with vulnerable Fortinet and FortiGate devices are encouraged to continue to monitor the Fortinet advisory website for patches and workarounds relating to CVE-2024-47575.

Where can I go for help?

If you suspect been impacted by this, we encourage you to submit a report at:

www.samcert.gov.ws/report-incident

If you require assistance with log analysis or are seeking advice on how to respond to this alert, please contact SamCERT directly:

✉ samcert@mcit.gov.ws

☎ +685 26 117