January 14, 2025

Arctic Wolf Uncovers Zero-Day Campaign Targeting Fortinet Firewalls

Overview: Arctic Wolf has revealed details of a sophisticated cyber campaign targeting Fortinet FortiGate firewalls with exposed management interfaces. Threat actors are exploiting a suspected zero-day vulnerability, enabling unauthorized administrative access to modify firewall configurations, extract credentials, and infiltrate networks. The attacks occurred in a multi-phase manner between November and December 2024, showcasing advanced techniques to compromise systems and evade detection.

CTI Analysis: The observed campaign demonstrates a strategic exploitation of FortiGate devices running firmware versions 7.0.14 to 7.0.16, released between February and October 2024. Attackers began with vulnerability scans and reconnaissance before escalating their activity to gain administrative control and extract sensitive credentials using the DCSync technique. To obscure their activities, they employed spoofed IP addresses, such as loopback and public DNS resolver addresses. The campaign highlights the evolving tactics of cybercriminals targeting exposed management interfaces and unpatched devices.

Impact Analysis: The attacks had widespread implications, enabling threat actors to achieve lateral movement and deeper infiltration into compromised environments. By leveraging administrative access, attackers modified firewall configurations, created new accounts, and established SSL VPN access for persistent control. The campaign, though opportunistic in nature, posed a severe risk to affected organizations by exposing sensitive credentials and network resources. The use of a suspected zero-day vulnerability amplifies the urgency for robust defensive measures.

Mitigation:

- Disable public access to FortiGate management interfaces immediately.
- Regularly update firewall firmware to the latest stable version to address vulnerabilities.
- Implement multifactor authentication (MFA) for all administrative access.
- Monitor for anomalous login behaviors, including unusual IP addresses or short-lived admin sessions.

- Conduct proactive threat hunting to detect unauthorized configuration changes or SSL VPN setups.

Conclusion: This campaign underscores the dangers of exposing management interfaces on public networks and the importance of staying vigilant against evolving cyber threats. Arctic Wolf's proactive measures and Fortinet's ongoing investigation into the zero-day vulnerability highlight the need for collaborative efforts to mitigate such risks. Organizations using FortiGate firewalls are strongly urged to act swiftly, secure their devices, and implement industry best practices to safeguard against future attacks.

Source:

https://cybersecuritynews.com/fortinet-fortigate-firewalls-under-attack-by-exploit-a-zero-day-vulnerability/

https://arcticwolf.com/resources/blog/console-chaos-targets-fortinet-fortigate-firewalls/