Campaign Targeting Firewalls and VPN Gateways Reported to Expose 70,000+ Credentials



Researchers describe a large-scale campaign against exposed edge devices, including Fortinet FortiGate and Palo Alto Networks GlobalProtect. Operators reportedly gained access to many organizations worldwide and tried to compromise some further.

- The campaign targets internet-exposed network edge devices.
- Named products include Fortinet FortiGate and Palo Alto Networks GlobalProtect firewalls.
- The headline reports more than 70,000 exposed credentials.
- Investigation artifacts indicate access to numerous organizations worldwide.
- Operators attempted further compromise of some victims.

What was reported

Researchers have published details of a large-scale campaign aimed at network edge devices that are reachable from the internet. The products named in the report include Fortinet FortiGate firewalls and Palo Alto Networks GlobalProtect. The report's headline puts the number of exposed credentials at more than 70,000.

According to the researchers, artifacts from the investigation indicate that the operators obtained access to numerous organizations worldwide and tried to compromise some of those victims further.

Why it matters

Firewalls and VPN gateways sit at the boundary of the network and often hold or process remote-access credentials. Access obtained at this layer can give an attacker a starting point for movement deeper into an environment. The source excerpt does not describe the technique used, any vulnerability identifiers, or which sectors or countries were affected, so institutions should avoid assuming a specific cause.

Suggested approach

Institutions that operate the named products, or any internet-facing remote-access gateway, should treat this as a prompt to review exposure and credential hygiene. The steps below are precautionary and do not depend on confirmation of a specific flaw.

What to do now

1. Inventory all internet-facing firewalls and VPN gateways, including any FortiGate and GlobalProtect devices.
2. Reset credentials used on edge devices and remote-access accounts, and enforce multi-factor authentication.
3. Review authentication and administrative logs on edge devices for unfamiliar logins or configuration changes.
4. Confirm devices run current vendor-supported firmware and restrict management interfaces from public exposure.
5. Check for signs of lateral movement from VPN-originated sessions and escalate findings through your incident process.