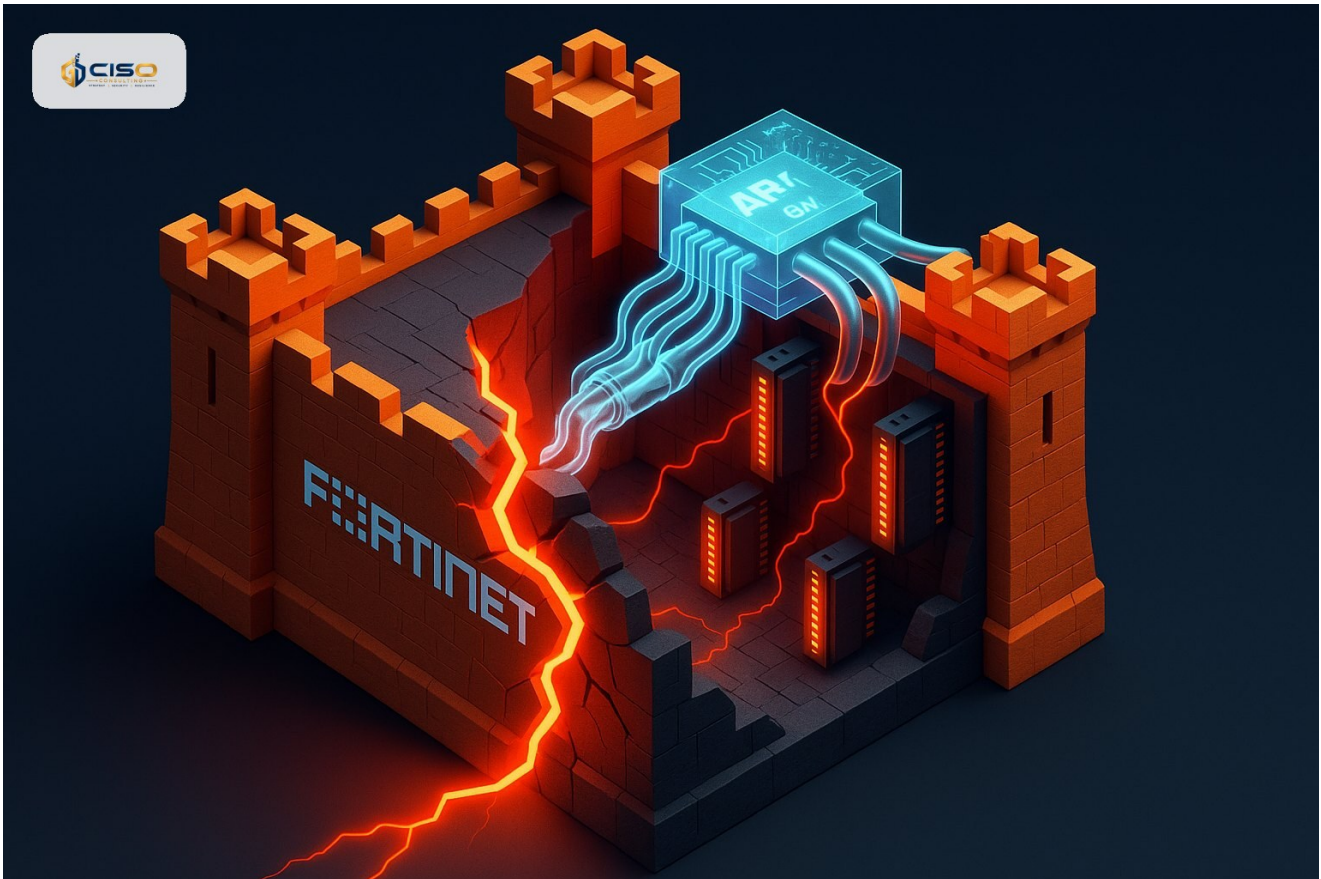


PEERSTITCH Malware Exploits FortiOS Path Traversal Flaw in Targeted Attacks



Advanced threat actors are exploiting a path traversal vulnerability in Fortinet FortiOS to deploy PEERSTITCH, a memory-resident ARM64 malware that bypasses security checks on VPN sessions.

- CVE-2025-61624 is a path traversal flaw in FortiOS, FortiPAM, FortiProxy and FortiSwitchManager command line interpreter with a CVSS score of 5.4
- PEERSTITCH is a previously unreported memory-resident ARM64 malware deployed through this vulnerability
- The malware bypasses security checks on tagged VPN sessions
- Attacks attributed to suspected advanced threat actors targeting Fortinet infrastructure

Vulnerability Details

A path traversal vulnerability tracked as **CVE-2025-61624** has been identified in the command line interpreter of multiple Fortinet products, including FortiOS, FortiPAM, FortiProxy, and FortiSwitchManager. The flaw carries a CVSS severity score of 5.4 and is being actively exploited by suspected advanced threat actors to compromise enterprise network infrastructure.

PEERSTITCH Malware Characteristics

Attackers are leveraging this vulnerability to deploy **PEERSTITCH**, a previously undocumented malware variant designed for ARM64 architectures. The malware operates as a memory-resident threat, making detection more challenging through traditional file-based scanning methods. A key capability of PEERSTITCH is its ability to bypass security checks on tagged VPN sessions, potentially allowing unauthorized access to protected network segments.

Implications for Saudi Institutions

Regulated institutions in the Kingdom operating Fortinet security appliances face elevated risk from this exploitation campaign. The targeting of VPN infrastructure is particularly concerning given the widespread reliance on remote access solutions across financial services, healthcare, and critical infrastructure sectors. Organizations should treat this as a priority patching event and conduct immediate verification of their Fortinet deployments. The memory-resident nature of the malware necessitates enhanced monitoring beyond standard endpoint detection approaches.

What to do now

1. Immediately inventory all Fortinet FortiOS, FortiPAM, FortiProxy and FortiSwitchManager deployments across the organization
2. Apply vendor-issued patches for CVE-2025-61624 on priority basis following change management procedures
3. Conduct memory forensics on all Fortinet appliances to detect potential PEERSTITCH infections
4. Review VPN session logs for anomalous tagged session activity and unauthorized access attempts
5. Enhance monitoring of Fortinet command line interpreter activity and implement behavioral detection rules
6. Coordinate with third-party security operations providers to verify integrity of managed Fortinet infrastructure