Check Point Firewalls and the Conflict Between the U.S. and Iran

Overview

Check Point Firewalls – CVE-2024-24919 VPN Vulnerability

- *CVE-2024-24919 (CVSS 8.6 out of 10)*
  - CVE-2024-24919 is a high-severity vulnerability affecting Check Point Security Gateways with Remote Access VPN or Mobile Access blades enabled. The flaw can allow unauthorized access to sensitive system files, such as /etc/shadow, which contain password hashes.
  - Exploitation does not require user interaction and has been actively observed in the wild since at least April 2024.
  - Iran-linked groups (like Pioneer Kitten, also known as UNC757) have been actively scanning the internet for vulnerable Check Point firewalls using this exact flaw.
  - The threat actors are targeting organizations in the U.S., Israel, and UAE, according to CISA, FBI, and private security firms. This is part of a broader Iranian strategy - exploiting VPN and firewall device vulnerabilities (e.g., Palo Alto CVE-2024-3400) to gain footholds in U.S. and allied infrastructure for espionage or ransomware operations
  - Iranian-linked scans include geolocation and industry verticals, meaning any exposed Check Point appliance is at risk.

CVSS Scoring System

The CVSS (Common Vulnerability Scoring System) is a standardized way to rate the severity of security vulnerabilities on a scale from 0 to 10, based on how easily a flaw can be exploited and the potential damage it can cause.

0.0–3.9 - Low

4.0–6.9 - Medium

7.0–8.9 - High

9.0–10.0 - Critical

A score of 8.6 means the vulnerability is high severity. It's serious, likely exploitable over the internet, doesn't need user interaction, and can lead to major compromise (like reading sensitive files or gaining unauthorized access).

While not the highest tier (critical), it demands urgent attention, especially if it's being actively exploited, like CVE-2024-24919.

- Check Point released a patch, but attackers were exploiting this vulnerability even before 2024, and exploitation is still happening now.

Victims

- Check Point Research reported attackers used the vulnerability to drop ShadowPad and NailaoLocker ransomware across European, African, and American organizations - primarily within the manufacturing sector.

- U.S. agencies (CISA, FBI, DOD) attribute scanning and potential exploit activity by Iranian-linked groups in regions like Israel, Azerbaijan, and the UAE.

Current Conflict Between the U.S. and Iran

- In the wake of the U.S. strikes on Iranian nuclear sites in June 2025, the Department of Homeland Security (DHS) issued a warning about possible cyber retaliation. Iranian-backed groups have a history of taking advantage of known vulnerabilities to gain access to U.S. systems, and CVE-2024-24919 remains one of the tools in their arsenal.

- There's no indication this specific vulnerability is being used in direct response to the conflict, but it continues to be exploited by the same threat actors who have a track record of tying cyber operations to geopolitical events. That makes it worth watching closely right now.

- In June 2025, the FBI and CISA warned in a joint advisory that Iranian government-backed threat actors and hacktivists are attempting to target U.S. defense contractors, industrial systems, and critical infrastructure via old, unpatched software vulnerabilities.

- There have been no confirmed large-scale attacks or coordinated campaigns, but the FBI and CISA encourage organizations to be on guard.
  - The U.S. is encouraging organizations to take proper precautions, such as:
    - Disconnecting OT and ICS systems from the internet
    - Patching software
    - Changing weak passwords
    - Requiring phishing-resistant multi-factor authentication

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may have exploited the Mobile Access/VPN blade on a Check Point firewall using CVE-2024-24919 to gain unauthorized file access.

Credential Access

- Unsecured Credentials: Credentials In Files [T1552.001] – The attacker may have accessed sensitive files like /etc/shadow to extract password hashes from the system.
- Steal Web Session Cookie [T1539] – If session tokens or cookies were retrieved, the attacker could hijack authenticated sessions to escalate access.

Persistence

- Server Software Component: Web Shell [T1505.003] – After initial exploitation, the attacker may upload a web shell to maintain remote access through the compromised firewall.

Command and Control

- Application Layer Protocol: Web Protocols [T1071.001] – If a web shell or other tool was deployed, communication with the attacker's C2 server may occur over HTTP/S to blend with normal traffic.

Targeted Industries

This Check Point vulnerability has been actively targeted across a wide range of sectors, especially those with exposed VPN infrastructure, including:

- Government and Defense – Local, national, and military networks have been scanned by nation-state groups.
- Finance – Banks, insurance providers, and financial services with remote access VPNs are high-value targets.
- Manufacturing – Confirmed ransomware infections linked to this exploit have hit manufacturing firms in multiple regions.
- Energy and Utilities – Critical infrastructure providers are top targets for both state and criminal actors.

- Technology and Telecom – VPN gateways in these environments are frequently targeted due to wide attack surfaces.

Supporting Documentation

sk182336 - Preventative Hotfix for CVE-2024-24919 - Quantum Gateway Information Disclosure

Attacks Surge on Check Point's Recent VPN Zero-Day Flaw

Check Point SSL VPN: CVE-2024-24919 from an Incident Response Perspective - Truesec

Advisory: Check Point Remote Access VPN vulnerability (CVE-2024-24919)

What's Going on With Check Point (CVE-2024-24919)? | GreyNoise Blog
Exposure Management Blog

Patch Now: Check Point Research Explains Shadow Pad, NailaoLocker, and its Protection - Check Point Blog

CPAI-2024-0353 - Check Point Software

US government warns of new Iran-linked cyber threats on critical infrastructure | Cybersecurity Dive

National Terrorism Advisory System Bulletin - June 22, 2025 | Homeland Security

What State and Local Governments Need to Know About Escalating Iran Cyber Threats