NO.DG-II/ CERT/4/124/2023
GOVERNMENT OF SINDH
SCIENCE & INFORMATION TECHNOLOGY
DEPARTMENT
Karachi, Dated: 13th November, 2025

To

1. The Chairman, Enquires, Anti-Corruption, Establishment Sindh, Karachi.
2. The Chairman, Planning & Development Board Sindh, Karachi
3. The Chairman/Chairperson, CMIT Sindh, Karachi
4. The Chairman Sindh HEC Karachi.
5. The Senior Member Board of Revenue (BOR)Sindh, Karachi.
6. The Additional Chief Secretary, Govt of Sindh_____.
7. The Principal Secretary to Governor Sindh, Governor Secretariat, Karachi.
8. The Principal Secretary to Chief Minister Sindh, Chief Minister Secretariat, Karachi.
9. The Administrative Secretary, Government of Sindh (All). _____.
10. The Provincial Ombudsman, Sindh.
11. The Inspector General of Police Sindh, Karachi
12. The Divisional Commissioner (All) in Sindh_____.

SUBJECT: **CYBERSECURITY ADVISORY ON IMMEDIATE MITIGATION OF MULTIPLE CRITICAL VULNERABILITIES IN PALO ALTO NETWORKS (PAN) PRODUCTS**

In view de recently identified multiple high-severity vulnerabilities in Palo Alto Networks (PAN) products which are being actively exploited by advanced persistent treat (AT groups, cyber-criminal syndicate and had actors the attached Advisory the NCA-15291025-National CERT Advisory-Multiple Critical Vulnerabilities in Polo Alto Network Annexure) has been issued by the National Cyber Emergency Response Team (National CERT).

2 The advisory outlines the nature, risks, and operational impacts of these vulnerabilities, which affect PAN-OS firewalls and associated cloud services. The identified flaws enable remote code execution (RCE), authentication bypass, and unauthorized administrative access allowing threat actors to gain full control of vulnerable systems. Ongoing exploitation campaigns have been observed globally and regionally since late 2024. Successful compromise may result in complete system takeover data theft espionage, persistent access, and disruption of critical security services.

3 Given the widespread deployment of PAN products across Pakistan's government, defence, financial, and critical infrastructure sectors, these vulnerabilities pose a serious National Cyber Security and data sovereignty threat. The advisory further highlights supply chain and vendor governance concerns urging all entities to conduct technology screening and ensure compliance with Pakistan Security Standards (PSS) to mitigate exposure

4 It is requested that the attached Advisory be disseminated to all relevant departments agencies, and organizations under your administrative control

Annexure: NCA-15291025-National CERT Advisory-Multiple Critical Vulnerabilities in Po Alto Networks (RAN) Products

(DR. RANA SHAHZAD QAISER)
DIRECTOR GENERAL-II
0310-2131415

A copy is forwarded for information and necessary action to:-

1. Director General (nCERT). L Block, Pak Secretariat, Islamabad.
2. AS(Staff) to Chief Minister Sindh, Karachi.
3. Director (Operations), S&IT Department, Govt. of Sindh
4. PS to Chief Secretary, Sindh.
5. Staff Officer to Special Assistant to Chief Minister Sindh, S&IT Department, Govt. of Sindh, Karachi.
6. PS to Secretary I&C, SGA&CD, Govt. of Sindh, Karachi.
7. Staff Officer to Secretary S&IT Department, Govt. of Sindh, Karachi.
8. Webmaster, for uploading the advisory on url: https://www.sindh.gov.pk/

Annexure

NCA-15.291025 – National CERT Advisory – Multiple Critical Vulnerabilities in Palo Alto Networks (PAN) Products

1. Introduction

Multiple high-severity vulnerabilities have recently been identified in Palo Alto Networks (PAN) products, including PAN-OS firewalls and associated services. These vulnerabilities have been actively exploited in the wild since late 2024 by state-sponsored threat actors, cybercriminal syndicates, and hacktivist groups. The flaws allow Remote Code Execution (RCE), authentication bypass, and unauthorized administrative access, posing a critical threat to enterprise and government network infrastructures globally.

Given PAN's extensive use in Pakistan's government, defense, and financial sectors, and its strategic cloud infrastructure presence through local partners, exploitation of these vulnerabilities presents a substantial national cybersecurity and data sovereignty risk.

2. Impact

Successful exploitation of these vulnerabilities may result in:

a. **Remote Code Execution (RCE):** Complete control of targeted PAN-OS systems or management interfaces.
b. **Privilege Escalation:** Unauthorized acquisition of administrator privileges, enabling configuration changes and data access.
c. **Credential Theft:** Extraction of stored authentication tokens and session data.
d. **Persistent Access:** Implantation of backdoors or malicious firmware for long-term espionage.
e. **Data Exfiltration:** Theft of sensitive data, including encrypted traffic, credentials, or configuration files.
f. **Service Disruption:** Degradation or denial of security services protecting critical infrastructure.
g. **Cloud Compromise:** Use of compromised firewalls as a pivot for lateral movement in hybrid or cloud environments.

3. Threat Details

3.1 Vulnerability Overview

CVE ID	Affected Product(s)	Description	CVSS v3.1	CWE
CVE-2024-0012	PAN-OS	Zero-day authentication bypass vulnerability enabling admin privilege escalation	9.8 (Critical)	CWE-287 (Improper Authentication)
CVE-2024-9474	PAN-OS	Exploited for remote access in cloud deployments	9.6 (Critical)	CWE-285 (Improper Authorization)
CVE-2025-0108	PAN Firewalls	Unauthorized access vulnerability exploited before patch release	8.7 (High)	CWE-306 (Missing Authentication for Critical Function)
CVE-2025-0282	Related PAN Services	Pre-authentication RCE potentially used for automated attacks	9.4 (Critical)	CWE-20 (Improper Input Validation)

3.2 Attack Complexity & Vector

a. **Attack Vector:** Remote (HTTP/HTTPS management interfaces, cloud APIs)
b. **Attack Complexity:** Low – requires only network access to vulnerable endpoint
c. **Privileges Required:** None (pre-authentication vulnerabilities)
d. **User Interaction:** Not required
e. **Exploitation Status:** Confirmed active exploitation in the wild since November 2024

3.3 Observed Activity

Security research teams including Arctic Wolf, Wiz, and Unit 42 have documented coordinated exploitation campaigns. Threat actors have leveraged compromised PAN-OS devices to gain initial access, move laterally within cloud environments, and deploy data-stealing implants. Attack telemetry indicates targeting of virtual firewall instances, cloud gateways, and internet-exposed NGFW management consoles.

Affected Systems

Systems vulnerable to these attacks include:

a. PAN-OS versions prior to the January 2025 patch (including 10.x and 11.x series).
b. Next-Generation Firewall (NGFW) appliances with exposed management interfaces.
c. Panorama management servers connected to cloud infrastructure.
d. Unsegmented or misconfigured deployments allowing public access to admin consoles.
e. Cloud-hosted PAN-OS instances used for hybrid environment connectivity.

5. Exploit Conditions

Successful exploitation typically requires:

a. Network access to exposed management or API interfaces.
b. Unpatched PAN-OS versions vulnerable to authentication bypass or RCE.
c. Absence of network segmentation isolating management networks.
d. Default or weak credentials remaining in production environments.
e. Direct internet exposure of firewall management ports (443, 4443, 6082).

6. Recommendations & Mitigation Actions

6.1 Patch Immediately (Primary Mitigation)

a. *Apply all latest PAN-OS and GlobalProtect updates as per the official Palo Alto Networks Security Advisory.*
b. *Validate the integrity of all firmware images and configuration backups.*
c. Reboot affected systems after patching and verify patch installation via version checks.

6.2 Restrict Access and Harden Configurations

a. Isolate management interfaces from the internet and restrict them to trusted subnets.
b. Disable unused services and web interfaces on PAN devices.
c. Change all administrative credentials, even after patching, to mitigate potential credential compromise.
d. Enforce multi-factor authentication (MFA) and least-privilege access controls.

6.3 Network and Endpoint Monitoring

a. Deploy Intrusion Detection/Prevention Systems (IDS/IPS) with updated PAN-OS signatures.
b. Monitor logs for unusual administrative logins, configuration changes, or file transfers.
c. Implement SIEM correlation rules for PAN management IPs and suspicious HTTP(S) POST requests.
d. Track indicators of compromise (IoCs) shared by Arctic Wolf and Wiz.

6.4 Supply Chain and Vendor Governance

a. Conduct vendor technology screening for cybersecurity products with potential foreign ownership or hostile affiliations.
b. Review contractual obligations and data residency clauses to ensure compliance with national security directives.
c. Integrate vendor assessment frameworks into procurement workflows for critical infrastructure.

6.5 Adoption of National Standards

a. Enforce compliance with the Pakistan Security Standards (PSS) for all ICT and cybersecurity procurements.
b. Vendors, partners, and government organizations with queries regarding certification and PSS compliance are urged to contact:
   - **Email**: asntisb1@cabinet.gov.pk
   - **Phone #** 051-9103543
c. Align PAN deployments with PSS guidelines for network segmentation, data sovereignty, and security auditing.
d. Require PSS certification for vendors operating in sensitive or government sectors.

6.6 Promote Indigenous Technologies

a. Prioritize local or sovereign cybersecurity solutions where feasible.
b. Support partnerships with domestic cybersecurity vendors for the development of indigenous firewall and cloud defense technologies.
c. Reduce dependency on foreign technologies for critical infrastructure protection.

6.7 Incident Preparedness and Response

a. Update incident response playbooks to include PAN-specific exploitation scenarios.
b. Immediately isolate compromised systems and collect forensic artifacts (logs, network captures, memory).
c. Notify National CERT and sectoral SOCs for coordinated incident response.
d. Verify backup integrity and restore from trusted images if compromise is confirmed.

7. Monitoring & Detection

Organizations should implement continuous monitoring for:

a. Repeated failed or successful admin logins from unrecognized IPs.
b. Configuration file modifications outside approved change windows.
c. Abnormal outbound connections initiated by PAN management interfaces.
d. Suspicious command execution patterns or system restarts.
e. Unusual API activity involving GlobalProtect or Panorama services.

Integrate findings into centralized SIEM platforms and correlate across network, endpoint, and cloud telemetry for early detection of compromise.

8. Incident Response & Readiness

If compromise is suspected:

a. Isolate affected PAN appliances immediately.
b. Preserve and analyze system logs, memory dumps, and network captures.
c. Reset credentials for all connected systems and administrators.
d. Validate firewall rules and access policies for unauthorized changes.
e. Conduct threat-hunting for persistence mechanisms, webshells, or lateral movement indicators.

9. Patching Summary

Version Category	Affected Components	Status
Vulnerable	PAN-OS prior to Jan 2025 patches; unsegmented or unpatched NGFWs	Must patch and harden immediately
Secure	Systems running latest PAN-OS builds with restricted management access	Continuous monitoring required

1. https://security.paloaltonetworks.com/CVE-2025-0108
2. https://nvd.nist.gov/vuln/detail/CVE-2025-0282
3. https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283?language=en_US

10. Call to Action

The National CERT strongly advises all government organizations, critical infrastructure operators, and financial institutions to:

a. Immediately patch all PAN-OS systems and verify configuration integrity.
b. Restrict management interfaces from public access and enforce strict access control.
c. Conduct comprehensive vendor and technology screening to eliminate dependencies on hostile-nation technologies.
d. Adopt Pakistan Security Standards (PSS) and promote indigenous security solutions for resilience.