NCA-11.170626 – National CERT Advisory

Critical Vulnerability in Palo Alto Networks GlobalProtect (CVE-2026-0257) Actively Exploited in the Wild

National CERT Pakistan has assessed an elevated cyber risk posture following confirmed in-the-wild exploitation of CVE-2026-0257, an authentication bypass vulnerability affecting the GlobalProtect portal and gateway components of Palo Alto Networks PAN-OS software.

The vulnerability may allow unauthenticated remote attackers to bypass security restrictions and establish unauthorized VPN connections, creating a pathway for initial access into enterprise and critical infrastructure environments.

This issue has been added to CISA's Known Exploited Vulnerabilities catalog, and organizations are advised to apply vendor patches, implement available mitigations, and immediately review relevant VPN and authentication logs for signs of compromise.

DOCUMENT SUMMARY

Field	Details
Advisory ID	NCA-11.170626
Threat Type	Authentication Bypass, Unauthorized VPN Access, Remote Network Exposure
Severity	High (CVE-2026-0257; actively exploited in the wild) https://nvd.nist.gov/vuln/detail/cve-2026-0257
Attack Vector	Remote network exploitation against GlobalProtect portal and gateway
Authentication Required	None
User Interaction	Not Required
CVSS Score	CVSS-BT 7.8 High (Palo Alto Networks CNA score)
Scope & Applicability	Government, financial sector, telecom, CII, and private enterprises using Palo Alto Networks GlobalProtect
Affected Condition	Especially relevant where authentication override cookies are enabled on vulnerable GlobalProtect deployments feed.craftedsignal+1
Products Not Impacted	Panorama and Cloud NGFW are not impacted

IMPACT ANALYSIS

Failure to remediate this vulnerability may result in:

1. **Unauthorized Network Access:** Attackers may establish VPN sessions without valid credentials.
2. **Initial Foothold in CII Networks:** Potential compromise of critical infrastructure environments.
3. **Lateral Movement Risk:** Expansion into internal enterprise networks post VPN access.
4. **Data Exfiltration Exposure:** Sensitive data theft from internal systems.
5. **Credential Harvesting:** Capture of authentication tokens and session data.
6. **Persistent Access Establishment:** Long-term foothold via compromised VPN infrastructure.
7. **Service Integrity Compromise:** Disruption of secure remote access services.
8. **Enterprise Network Reconnaissance:** Mapping of internal systems via VPN access.
9. **Operational Disruption:** Potential downtime due to incident response and containment.
10. **National Cybersecurity Impact:** Risk to interconnected government and enterprise systems.

THREAT CHARACTERISTICS

Characteristic	Details

Threat Category	Exploited Network Perimeter Vulnerability
Threat Status	Active Exploitation (Global Campaigns Observed)
Root Cause	Authentication Bypass in GlobalProtect PAN-OS Components
Target Scope	Government, Enterprise Networks, CII, Financial Institutions
Attack Complexity	Low (Once Exploit is Available)
Privileges Required	None
Affected Systems	Palo Alto Networks PAN-OS GlobalProtect Portals and Gateways
CWE Classes	CWE-287 (Improper Authentication), CWE-306 (Missing Authentication), CWE-288 (Authentication Bypass)

INDICATORS OF EXPOSURE / TARGETING (IoEs)

Organizations should immediately search GlobalProtect and VPN logs for the following indicators:

1. Suspicious Source IP Activity

- 23.128.228[.]6
- 104.207.144[.]154
- 146.19.216[.]119
- 146.19.216[.]120
- 146.19.216[.]125
- 179.43.172[.]213
- 185.195.232[.]139
- 198.12.106[.]60
- 202.144.192[.]47

2. Suspicious Host Identifiers

- aa:bb:cc:dd:ee:ff (MAC address indicator)
- 00:11:22:33:44:55 (MAC address indicator)
- WINDOWS-LAPTOP-001
- DESKTOP-GP01
- GP-CLIENT

3. Exploitation Artifacts (PoC-Linked Indicators)

- endpoint_os_version: Microsoft Windows 10 Pro 64-bit
- source_user_info.domain: (empty / null value observed in exploit flow)

4. Behavioral Indicators

- Successful VPN logins without corresponding authentication events
- Gateway-connected sessions without credential validation logs
- Short-duration unauthorized VPN sessions
- Logins originating from anomalous or high-risk IP ranges

REMEDIATION ACTIONS

1. Immediate Defensive Controls

Action Category	Specific Actions
Patch Management	Upgrade PAN-OS to vendor-patched versions immediately
Mitigation	Apply Palo Alto Networks security advisory workarounds
Access Control	Restrict GlobalProtect exposure to trusted IPs

MFA Enforcement	Enforce MFA for all remote access users
Logging	Enable enhanced VPN authentication logging
Session Control	Terminate suspicious or unknown active sessions

2. Enhanced Monitoring & Detection

Tool / Control	Purpose
SIEM Correlation Rules	Detect anomalous VPN authentication patterns
VPN Log Analysis	Identify unauthenticated session creation attempts
Threat Intelligence Feeds	Detect known malicious IPs and exploitation clusters
Behavioral Analytics	Identify abnormal VPN usage patterns
Network Monitoring	Detect post-exploitation lateral movement

3. Incident Response Requirements

Organizations must:

- Immediately investigate any successful or suspicious GlobalProtect gateway connections
- Correlate VPN logs with firewall and authentication logs
- Isolate potentially compromised endpoints
- Conduct credential rotation for affected users
- Preserve logs for forensic analysis

ACTION SUMMARY & RESPONSE PRIORITIES

Action Type	Specific Steps	Priority
Patch Deployment	Upgrade PAN-OS immediately	**CRITICAL**
Threat Monitoring	Enable enhanced VPN log analysis	**CRITICAL**
IOC Hunting	Search listed IPs and host indicators	**CRITICAL**
Session Review	Audit active VPN sessions	**HIGH**
Credential Reset	Rotate affected credentials	**HIGH**
Incident Reporting	Escalate suspected compromise	**HIGH**

MONITORING & DETECTION REQUIREMENTS

1. Monitor unauthorized VPN authentication attempts
2. Detect anomalous GlobalProtect gateway sessions
3. Identify login attempts from listed malicious IPs
4. Track session creation without authentication logs
5. Monitor unusual geographic access patterns
6. Detect credential-less authentication flows
7. Validate VPN log integrity
8. Monitor for post-exploitation lateral movement
9. Identify abnormal outbound traffic from VPN users
10. Correlate firewall and VPN authentication logs

INCIDENT REPORTING

All suspected compromise, anomalous VPN activity, or exploitation attempts must be immediately reported to National CERT Pakistan:

- **Incident Reporting Portal:** https://pkcert.gov.pk/report-incident/
- **Email:** cert@pkcert.gov.pk
- **UAN:** +92 519203412

CALL TO ACTION – KEY IMPERATIVES

#	Requirement
1	Apply security patches immediately
2	Monitor GlobalProtect authentication logs
3	Investigate listed IoCs without delay
4	Enforce MFA across all remote access
5	Terminate suspicious VPN sessions
6	Conduct rapid compromise assessment
7	Escalate confirmed anomalies to National CERT
8	Strengthen perimeter VPN security controls

ADVISORY NOTE: Organizations operating Palo Alto Networks GlobalProtect infrastructure are strongly advised to treat this vulnerability as an active exploitation scenario. Immediate remediation, continuous monitoring, and proactive threat hunting are essential to prevent unauthorized remote access and potential compromise of critical internal networks.