NCA-12.180626 – National CERT Advisory

Large-Scale Compromise of Fortinet FortiGate Firewalls and VPN Infrastructure

National CERT Pakistan has assessed an elevated cyber risk posture following the discovery of a large-scale global cyber intrusion campaign targeting internet-exposed Fortinet FortiGate firewalls and VPN gateways. Security researchers have identified evidence of widespread compromise affecting approximately 73,932 Fortinet firewall instances across 194 countries, resulting in exposure of credentials and unauthorized access to enterprise and critical infrastructure environments.

The campaign is believed to involve organized cybercriminal operators conducting large-scale credential harvesting, brute-force attacks, VPN credential cracking, and post-compromise lateral movement activities. Analysis indicates that exposed FortiGate management interfaces and legacy credential storage mechanisms were leveraged to obtain administrative access and establish persistent footholds within victim networks.

Given the scale, sophistication, and active exploitation observed, organizations utilizing Fortinet FortiGate infrastructure are advised to immediately assess their exposure, implement remediation measures, and conduct threat hunting activities.

DOCUMENT SUMMARY

Field	Details
Advisory ID	NCA-12.180626
Threat Type	Firewall Compromise, Credential Theft, VPN Breach, Initial Access Operations
Severity	Critical
Attack Vector	Internet-exposed FortiGate Management Interfaces and VPN Infrastructure
Authentication Required	None (for exposed interfaces and compromised credentials)
User Interaction	Not Required
Scope & Applicability	Government, Financial Sector, Telecom, Energy, Healthcare, Education, Critical Information Infrastructure (CII), and Private Enterprises using Fortinet FortiGate devices
CVSS Score	N/A
Affected Condition	Publicly accessible FortiGate management interfaces, weak credential protection, legacy password hashing configurations
Products Affected	Fortinet FortiGate Firewalls and SSL VPN Deployments
Threat Status	Active Global Campaign

IMPACT ANALYSIS

Failure to investigate and remediate exposure may result in:

1. Unauthorized Administrative Access to firewall management infrastructure.
2. Compromise of VPN Gateways enabling attacker entry into internal networks.
3. Theft of Administrative Credentials and configuration data.
4. Active Directory Compromise through post-exploitation lateral movement.
5. Persistent Backdoor Access established within enterprise environments.
6. Data Exfiltration involving sensitive corporate and government information.
7. Security Control Manipulation through modification of firewall policies.
8. Supply Chain Risk through compromise of third-party and vendor access.
9. Operational Disruption affecting business continuity and critical services.
10. National Cybersecurity Impact involving interconnected government and critical infrastructure systems.

THREAT CHARACTERISTICS

Characteristic	Details
Threat Category	Compromised Network Perimeter Infrastructure
Threat Status	Active Global Exploitation Campaign
Root Cause	Exposed Management Interfaces and Credential Compromise
Target Scope	Government, Enterprise Networks, Critical Infrastructure, Telecommunications, Financial Institutions
Attack Complexity	Moderate
Privileges Required	None (Initial Access Phase)
Affected Systems	Fortinet FortiGate Firewalls and SSL VPN Gateways
Attack Scale	Approximately 73,932 Compromised Firewall URLs Across 194 Countries
Observed Adversary Activity	Credential Theft, Hash Cracking, Lateral Movement, Data Exfiltration
Persistence Mechanisms	Backdoor Accounts, Modified Security Policies, Active Directory Access

INDICATORS OF EXPOSURE / TARGETING (IoEs)

Organizations should immediately investigate the following conditions:

1. Administrative Access Indicators

- Successful administrator logins from unusual geographic locations.
- Administrative sessions occurring outside business hours.
- Newly created administrator accounts.
- Unexpected privilege changes for existing accounts.

2. VPN Indicators

- Successful SSL VPN logins from unfamiliar IP addresses.
- Repeated authentication attempts followed by successful access.
- VPN sessions associated with dormant or inactive accounts.
- Unusual VPN usage patterns.

3. Firewall Configuration Indicators

- Unauthorized changes to security policies.
- Unexpected firewall rule modifications.
- Newly added trusted IP addresses.
- Disabled security controls or monitoring features.

4. Active Directory Indicators

- Unexpected domain administrator activity.
- New privileged user creation.
- Excessive authentication requests.
- Lateral movement activity originating from firewall-associated systems.

5. Network Activity Indicators

- Unusual outbound connections.
- Large-volume data transfers.

- Communications with unknown external infrastructure.
- Reconnaissance and internal scanning activity.

HIGH-RISK SECTORS OBSERVED

The campaign impacted organizations across multiple sectors, including:

- Government Services
- Telecommunications
- Information Technology Services
- Financial Services
- Healthcare
- Education
- Manufacturing
- Industrial Automation
- Critical Infrastructure
- Logistics and Transportation
- Legal Services
- Professional Consulting

REMEDIATION ACTIONS

1. Immediate Defensive Controls

Action Category	Specific Actions
Exposure Reduction	Remove FortiGate Management Interfaces from public internet access
Patch Management	Upgrade to latest supported FortiOS releases
Credential Security	Force immediate password reset for all administrative accounts
Password Hashing	Ensure administrators log in after upgrades to enable PBKDF2 credential storage
MFA Enforcement	Implement MFA on all administrative and VPN accounts
Access Control	Restrict management access to trusted networks only
Configuration Review	Audit firewall policies and administrator accounts
Threat Hunting	Review logs for indicators of compromise

2. Enhanced Monitoring & Detection

Tool / Control	Purpose
SIEM Correlation Rules	Detect abnormal administrative access
VPN Log Monitoring	Identify unauthorized VPN activity
Threat Intelligence Feeds	Detect known malicious infrastructure
Behavioral Analytics	Identify anomalous administrator behavior
Network Monitoring	Detect lateral movement and exfiltration
Firewall Audit Logging	Track unauthorized configuration changes
Identity Monitoring	Detect compromised administrative accounts

3. Incident Response Requirements

Organizations must:

- Assume compromise if suspicious administrator logins are identified.
- Conduct a full review of firewall configurations.

- Identify unauthorized administrator accounts.
- Review VPN authentication logs.
- Investigate Active Directory for signs of lateral movement.
- Rotate all administrator and service account credentials.
- Rebuild or replace devices where compromise cannot be confidently ruled out.
- Preserve logs and forensic evidence for investigation.

ACTION SUMMARY & RESPONSE PRIORITIES

Action Type	Specific Steps	Priority
Exposure Reduction	Remove public management interface access	**CRITICAL**
Credential Rotation	Reset all administrator credentials	**CRITICAL**
MFA Enforcement	Enable MFA across administrative systems	**CRITICAL**
Threat Hunting	Review logs for unauthorized access	**CRITICAL**
Configuration Audit	Validate firewall and VPN settings	**HIGH**
Active Directory Review	Investigate lateral movement indicators	**HIGH**
Incident Reporting	Escalate confirmed compromises	**HIGH**
Continuous Monitoring	Enable enhanced detection controls	**HIGH**

MONITORING & DETECTION REQUIREMENTS

1. Monitor administrator login activity.
2. Detect unauthorized VPN access attempts.
3. Identify abnormal geographic login patterns.
4. Monitor firewall configuration changes.
5. Detect creation of unauthorized administrator accounts.
6. Monitor Active Directory privilege escalation activity.
7. Detect internal reconnaissance and scanning.
8. Monitor outbound data transfers.
9. Correlate firewall, VPN, and identity logs.
10. Investigate persistence and backdoor indicators.

INCIDENT REPORTING

All suspected compromise, unauthorized administrative access, firewall manipulation, VPN abuse, or related malicious activity should 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	Remove internet exposure of FortiGate management interfaces
2	Upgrade FortiOS to supported versions immediately
3	Force password rotation for all administrators
4	Ensure migration to PBKDF2 credential protection
5	Enforce MFA on VPN and administrative access
6	Conduct compromise assessment and threat hunting
7	Review firewall and VPN logs for suspicious activity
8	Audit Active Directory for lateral movement indicators
9	Investigate unauthorized configuration changes
10	Report confirmed incidents to National CERT Pakistan

ADVISORY NOTE: Organizations operating Fortinet FortiGate firewalls and SSL VPN infrastructure should treat this incident as a potential compromise scenario rather than a routine vulnerability management issue. Given the scale of the campaign, the prevalence of credential theft, and the observed post-compromise activity, immediate remediation, credential rotation, threat hunting, and continuous monitoring are strongly recommended to prevent unauthorized access to enterprise and critical infrastructure networks.