NO.DG-II/ Cyber Advisory/4/111/2023
GOVERNMENT OF SINDH
SCIENCE & INFORMATION TECHNOLOGY DEPARTMENT

Karachi, Dated 23th May, 2025

To

1. The Chairman, Enquires, Anti-Corruption, Establishment Sindh, Karachi.
2. The Chairman, Planning & Development Board Sindh, Karachi
3. The Chairman/Chairperson, Chief Minister Inspection Enquiries and Implementation Team 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_____
13. The Deputy Commissioner, District _____

SUBJECT: CYBER SECURITY ADVISORY FORTINET FIREWALL VULNERABILITIES EXPLOITED BY LOCKBIT-LINKED RANSOMWARE GROUP (ADVISORY NO. 07/2025)

A ransomware group associated with LockBit, identified as Mora_001 has been actively exploiting critical vulnerabilities in Fortinet's FortiOS and FortiProxy products. These exploits have facilitated unauthorized access to systems, leading to the deployment of a custom ransomware strain Known as SuperBlack. The attacks have been ongoing since late January 2025, targeting organizations with exposed FortiGate firewalls. Consequently, Fortinet has issued patches and urges users to update accordingly.

2 Technical Details

a. Vulnerabilities Involved.

(1) **CVE-2024-55591** Critical authentication bypass vulnerability affecting FortiOS versions 7.0.0 through 7.0.16 and FortiProxy versions 7.0.0 through 7.2.19 and 7.0.2 through 7.0.12. This flaw allows remote attackers to gain super-admin privileges via crafted request to the Node.js WebSocket module enabling unauthorized code or command execution.

(2) **CVE-2025-24472**. A related high-severity authentication bypass vulnerability affecting the same product versions. It was reported by victims of attacks investigated by Forescout and is addressed by the same patch that resolves CVE-2024-55591

b. Attack Methodology

(1) Exploitation of the aforementioned vulnerabilities to gain unauthorized access with super super-admin privileges.
(2) Creation of new privileged accounts with names such as forticloud-tech, fortigate-firewall and administrator.
(3) For firewalls with VPN capabilities, creation of local user accounts mimicking legitimate users to maintain persistent access.
(4) Utilization of high availability (HA) configuration propagation to compromise additional firewalls within the same cluster.
(5) Deployment of the SuperBlack ransomware, a variant based on the LockBit 3.0 builder, featuring data exfiltration for double extortion and a custom wiper tool to erase traces of the ransomware executable.

3. **Recommendations**. All Fortinet administrators/users are urged to update their products as

a. Upgrade FortiOS to version 7.0.17 or later.
b. Upgrade Forti Proxy to version 7.2.13 or later or 7.0.20.
c. Remove the firewall's web-based management interface from public internet exposure.
d. Regularly review administrative accounts for unauthorized additions or changes.
e. Monitor for unexpected configuration changes and unauthorized login attempts.
f. Be vigilant for indicators of compromise, such as unusual automation tasks or unexpected VPN connections.
g. Implement strict network segmentation to limit lateral movement opportunities for attackers.
h. Enforce multi-factor authentication (MFA) for all administrative access.

4 Kindly disseminate the above information to all concerned in your organization, attached/affiliated departments and ensure necessary protective measures.

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

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

1. AS(Staff) to Chief Minister Sindh, Karachi.
2. The Assistant Secretary (NTISB), Cabinet Secretariat, Cabinet Division (NTISB), GoP.
3. PS to Chief Secretary, Sindh.
4. PS to Secretary I&C, SGA&CD, Govt. of Sindh, Karachi.
5. Staff Officer to S&IT Department, Govt. of Sindh, Karachi.
6. Webmaster, for uploading the advisory on url: *https://www.sindh.gov.pk/*