No.10 (6)/2016-Coord
Government of Pakistan
Ministry of Science and Technology
******

Islamabad, the 19th May, 2025

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

Enclosed please find herewith Cabinet Division's U.O No.1-5/2023/24(NTISB-II) dated 16th May, 2025 on the subject cited above. The content of the letter is reproduced under for strict compliance, please.

Context. A ransomware group associated with Lock Bit, 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 Super Black. 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 7.0.19 and 7.2.0 through 7.2.12. This flaw allows remote attackers to gain super-admin privileges via crafted requests 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 mentioned below:

a. Upgrade FortiOS to version 7.0.17 or later.

b. Upgrade FortiProxy 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.

2. This message is to all concerned in your organization for ensuring necessary protective measures, Please.

Encl: As above.

(RIDA NOOR)
Section Officer (Coord)
Tel: 9202520

Distribution:

All Head of Organizations

Copy for information to:

All Heads of Wing, MoST

Central Registry NUTECH	
Rector	
Pro-Rector	
Dy Dir (Coord)	
GSO-1 (Coord)	
Head Clk	
Dte/Office	ICT
Diary No	
Date	19/5/25

ICT

Please share with all