Subject: - **Cyber Security Advisory - Fortinet Releases Critical Patch Update (Advisory No. 56)**

Context. Fortinet has patched a zero-day vulnerability in its products having FortiOS SSL VPN. The vulnerability (CVE-2022-42475) is a heap-based buffer overflow bug that could allow unauthenticated users to crash devices remotely and potentially perform code execution. Users and Administrators are requested to examine and apply necessary updates as per recommendation mentioned at para-2.

2. **Recommendations**

a. For detailed information regarding vulnerability of IT/Network, admins are advised to visit https://fortiguard.com/psirt/FG-IR-22-398.

b. Fortinet has released patches for following versions: -

(1) FortiOS version 7.2.3 or above.

(2) FortiOS version 7.0.9 or above.

(3) FortiOS version 6.4.11 or above.

(4) FortiOS version 6.2.12 or above.

(5) FortiOS-6k7k version 7.0.8 or above.

(6) FortiOS-6k7k version 6.4.10 or above.

(7) FortiOS-6k7k version 6.2.12 or above.

(8) FortiOS-6k7k version 6.0.15 or above.

c. Further details on subject vulnerabilities and related patches may be acquired from FortiGuard Labs (FG-IR_22-398).

3. Kindly disseminate the above message to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.