NO.DG-II/ CERT/4/124/2023
GOVERNMENT OF SINDH
SCIENCE & INFORMATION TECHNOLOGY DEPARTMENT
Karachi, Dated: 19th December, 2025

To

1. The Chairman, Enquires, Anti-Corruption, Establishment Sindh, Karachi.
2. The Chairman, Planning & Development Board Sindh, Karachi
3. The Chairman/Chairperson, CMIT 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_____.

SUBJECT: CYBERSECURITY ADVISORY ON PREVENTION AGAINST EXPLOITATION OF VIDEO CONFERENCING APPLICATIONS (ZOOM. GOOGLE MEET. ETC.)

In view of the Increasing Cyber threats targeting video conferencing platforms, including Zoom, Google Meet, (and similar services, the attached Advisory titled "NCA 19.101225-National CERT Advisory Cybersecurity Advisory on Prevention Against Exploitation of Video Conferencing Applications (Zoom, Google Meet, etc) **(Annexure-A)** has been issued by **the National Cyber Emergency Response Team (National CERT)**. A Representative CVE Threat Matrix **(Annexure-B)** is attached, containing example CVEs for each threat category, CVSS scores, and attack vectors. This Annex is intended for SOC/IR teams to enhance technical understanding and facilitate Internal risk assessments.

2. The advisory outlines the nature, risks, and operational impacts associated with video conferencing platforms including unauthorised access, data leakage, endpoint compromise, API exploitation, and service disruption. These threats have been observed globally and locally, emphasizing the critical need for implementing security best practices to safeguard sensitive communications.

3. Given the widespread use of these platforms across Pakistan's government, defense, financial, and critical infrastructure sectors, the risks posed by insecure video conferencing practices are significant. The advisory provides actionable recommendations to prevent unauthorised access, ensure secure host and endpoint configurations, implement multi-layered defenses, and maintain the confidentiality and integrity of organizational communications.

4 It is requested that the attached Advisory and Annex-B be disseminated to all relevant departments, agencies, and organizations under your administrative control to ensure **timely implementation of the recommended security measures.**

Annexure-A: NCA-19.101225 National CERT Advisory Cyber Security Advisory on Prevention Against Exploitation of Video Conferencing Applications (Zoom, Google Meet, etc.)
Annexure-B: Representative CVE Threat Matrix for internal SOC/IR Teams.

"Disclaimer: This Document contains confidential information and it is not to be disclosed to media or any public information platform."

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

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

1. Chief Executive Officer Sindh IT Company (SITC), Karachi.
2. Director General (nCERT). L Block, Pak Secretariat, Islamabad
3. PS(Staff) to Chief Minister Sindh, Karachi.
4. Director (Operations), S&IT Department, Govt. of Sindh
5. PS to Chief Secretary, Sindh.
6. Staff Officer to Special Assistant to Chief Minister Sindh, S&IT Department, Govt. of Sindh, Karachi.
7. PS to Secretary I&C, SGA&CD, Govt. of Sindh, Karachi.
8. Staff Officer to Secretary S&IT Department, Govt. of Sindh, Karachi.
9. Webmaster, for uploading the advisory on url: *https://www.sindh.gov.pk/*

Annexure A

NCA-19.101225 – National CERT Advisory – Cyber Security Advisory on Prevention Against Exploitation of Video Conferencing Applications (Zoom, Google Meet, etc.)

1. Introduction

Increasing reliance on video conferencing platforms such as Zoom, Google Meet, and others has led to a rise in cyber-attacks targeting these services. Multiple incidents of unauthorized access ("Zoom-bombing"), account compromise, data leakage, and exploitation of vulnerabilities have been reported in recent months.

These platforms, if misconfigured or used without proper security controls, are susceptible to hacking, data exfiltration, denial-of-service attacks, and compromise of endpoint devices. The advisory provides essential security best practices to ensure safe and secure use of online video conferencing tools within government and enterprise environments.

Representative CVE Threat Matrix (Annexure B) for internal SOC/IR teams with CVSS scores and attack vectors is also attached.

2. Impact

Successful exploitation of video conferencing applications may result in:

a. **Unauthorized Access** – Intruders joining confidential meetings.
b. **Data Theft or Leakage** – Exposure of sensitive information shared visually, verbally, or via chat.
c. **Endpoint Compromise** – Attacks targeting operating systems of devices running conferencing software.
d. **Service Disruption** – DoS/DDoS attacks resulting in meeting downtime.
e. **API/Interface Abuse** – Exploitation of management interfaces or server APIs for broader compromise.

3. Threat Details

3.1 Threat & Vulnerability Overview

Cyber security concerns associated with video conferencing platforms include:

Threat Category	Description	Severity	CVSS Score
Account Hacking	Compromise due to weak passwords or insecure meeting settings.	High	7.5
Data Leakage / Zero-day Exploits	Exploitation of platform vulnerabilities or unpatched software.	Critical	9.0
Endpoint Attacks	Malware or targeted attacks on host operating systems.	High	8.0
Server-Side Attacks	Abuse of management interfaces or APIs of video conferencing servers.	Critical	9.1
DoS/DDoS Attacks	Flooding of conferencing servers to disrupt communication.	High	7.8

Note: Severity ratings map to CVSS scoring ranges (High ≈ 7.0–8.9, Critical ≈ 9.0–10.0), and organizations should maintain an internal technical matrix containing full CVE and CVSS data for accurate risk alignment.

4. Attack Complexity & Vector

a. **Attack Vector:** Remote (internet-exposed meeting links, API endpoints, or unprotected sessions)
b. **Attack Complexity:** Low to moderate depending on platform configuration
c. **Privileges Required:** None for meeting intrusion; higher for system-level compromise
d. **User Interaction:** Required (joining meetings, sharing screens, accepting links)
e. **Exploitation Status:** Increasingly reported across global organizations

5. Affected Systems

The following environments are most at risk:

a. Video conferencing platforms configured with weak or default security settings

b. Systems without the latest application or OS security updates
c. Organizations sharing meeting links publicly or through insecure channels
d. Installations lacking endpoint protection or proper system hardening
e. Servers exposed to untrusted networks, including publicly accessible APIs

6. Exploit Conditions

Exploitation is more likely when:

a. Meeting links or credentials are shared on open forums or social media
b. Waiting room/lobby features are disabled
c. Screen sharing is allowed for all participants
d. Host or participant devices lack endpoint security
e. Video conferencing servers run outdated or vulnerable software
f. Organizations use single-vendor stacks without layered security defenses

7. Recommendations & Mitigation Actions

7.1 Strengthen Meeting Security Settings

a. Share meeting information only with authorized individuals through secure email or private VoIP messaging
b. Issue meeting IDs shortly before the session begins
c. Enable and enforce Waiting Room/Lobby features
d. Lock meetings once all intended participants have joined
e. Restrict screen sharing to the host by default
f. **Meeting links should be treated as sensitive credentials and shared only via authenticated and secure channels to mitigate account compromise risks.**

7.2 Secure Hosts & Endpoint Systems

a. Ensure endpoint protection and system hardening for all hosts
b. Regularly update video conferencing applications and operating systems
c. Avoid using online meeting tools for sharing classified or sensitive data

7.3 Apply Organizational Security Controls

a. Use multi-layered and multi-vendor security solutions in sensitive environments
b. Segment networks hosting conferencing systems
c. Deploy monitoring solutions (IDS/IPS/SIEM) to detect anomalies
d. Limit external access to conferencing servers or management interfaces

e. Organizations should deploy layered defenses using endpoint protection, network segmentation, and application-level controls to ensure full-stack risk mitigation across conferencing environments.

8. Monitoring & Detection

Organizations should actively monitor:

a. Unauthorized or unknown participants joining meetings
b. Sudden screen-sharing attempts by non-host users
c. Unusual API requests or access to management interfaces
d. Spikes in network traffic indicating DoS/DDoS activity
e. Signs of sensitive data being copied, recorded, or exfiltrated
f. Unexpected behavior on devices used for hosting meetings

9. Incident Response & Readiness

a. Immediately remove unauthorized participants and lock meetings
b. Report suspicious files, emails, intrusions, or hacking attempts
c. Conduct forensic analysis of compromised systems (logs, memory, artifacts)
d. Verify integrity and configuration of conferencing platforms
e. Maintain secure and tested backups of system configurations

10. Reporting Suspicious Activity

Organizations are advised to report all cyber incidents, suspicious files, or hacking cases to the National CERT:

- **Email:** cert@pkcert.gov.pk
- **Incident Reporting Portal:** https://pkcert.gov.pk/report-incident
- **Fax:** +92-51-9203412

11. Call to Action

The National CERT urges all organizations to:

a. Implement the recommended security controls immediately
b. Enforce strict meeting access and host-level controls
c. Keep all conferencing systems and endpoints up to date
d. Continuously monitor for unauthorized access or suspicious activity

6. Integrate video conferencing security into organizational cyber risk management practices.

Act now – secure your video conferencing environments before a cyber attacker takes advantage of these vulnerabilities.