NO.DG-II/ CERT/4/124/2023
GOVERNMENT OF SINDH
SCIENCE & INFORMATION TECHNOLOGY
DEPARTMENT
Karachi, Dated: 17th 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 RISKS ASSOCIATED WITH SMART / INTERNET-ENABLED IPTV DEVICES IN SENSITIVE PREMISES IMMEDIATE MITIGATION MEASURES**

In light of the Cybersecurity risks associated with Smart/Internet-Enabled IPTV devices deployed within sensitive office environments, the attached Advisory titled "NCA-18 101225-National CERT Advisory - Security Risks Associated with Smart/Internet-Enabled IPTV Devices in Sensitive Premises" **(Annexure A)** has been issued by the National Cyber Emergency Response Team (National CERT). Additionally, **(Annexure-B)** containing the CVE-aligned threat matrix has been included to support technical teams in assessing associated vulnerabilities.

2. The advisory outlines significant vulnerabilities arising from the presence of **Smart/Internet-Enabled IPTV devices** equipped with microphones, cameras, network connectivity, and complex operating systems. These features have been assessed as potential vectors for unauthorised surveillance. network infiltration, malware deployment, and data ex-filtration. Instances have been observed where inadequate isolation, outdated software, and insecure configurations increased the risk of compromise, particularly in areas where sensitive or classified discussions occur.

3. The risks highlighted underscore the security concerns associated with internet-enabled audiovisual equipment deployed in strategic workspaces, including conference rooms, operation centers, and senior leadership offices.

4. It is requested that the attached Advisory be disseminated to all relevant departments. agencies, and organisations under your administrative purview for immediate compliance with the recommended mitigation measures, including discontinuation of Smart / Internet-Enabled IPTV devices in designated sensitive zones and implementation of enhanced monitoring and control mechanisms

Annexure-A: NCA-18.101225-National CERT Advisory - Security Risks Associated with Smart/ Internet –Enabled IPTV Devices in Sensitive Premises.
Annexure-B: Threat Matrix for Smart /Internet –Enabled IPTV Device Risk Context.

"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. AS(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-18.101225 – National CERT Advisory – Security Risks Associated with Smart / Internet-Enabled IPTV Devices in Sensitive Premises

1. Introduction

Significant cybersecurity risks associated with the use of **Smart / Internet-Enabled IPTV devices** in sensitive office environments have been identified. **This advisory addresses class-level risks inherent to this category of devices, rather than product-specific or CVE-specific vulnerabilities.** These devices, commonly used for presentations, broadcasting, and communication, introduce multiple attack vectors due to their integrated microphones, cameras, wireless connectivity, and complex operating systems.

Recent analyses and incidents demonstrate that compromised **Smart / Internet-Enabled IPTV devices** can enable unauthorized surveillance, network infiltration, malware deployment, and data exfiltration. When installed in conference rooms, leadership offices, operations centers, or other sensitive zones, these devices pose a substantial threat to organizational information security and may enable targeted espionage or operational compromise.

Given their widespread deployment and inherent vulnerabilities, immediate risk mitigation is required.

(For technical teams, a CVE-aligned threat matrix is included as **Annex-B**)

2. Impact

Successful compromise of **Smart / Internet-Enabled IPTV devices** may result in:

a. **Remote Surveillance** – Covert activation of microphones/cameras enabling live monitoring or recording of sensitive discussions.
b. **Network Infiltration** – Use of the TV as a pivot point for lateral movement into internal networks.
c. **Malware Deployment** – Injection of malware or ransomware into the device to establish persistent access.
d. **Unauthorized Data Exfiltration** – Leakage of screen content, meeting information, credentials, and network metadata.
e. **Operational Breach** – Compromise of strategic meetings, command centers, or restricted-information workspaces.

3. Threat Details

3.1 Threat Overview

Threat Category	Description	Severity
Remote Surveillance	Covert activation of microphones/cameras to monitor meetings	High
Network Infiltration	Exploitation of open ports and insecure services for internal network access	High
Malware Deployment	Installation of malicious software via insecure OS or firmware	High
Data Exfiltration	Unauthorized transmission of sensitive information through compromised devices	High

3.2 Attack Complexity & Vector

- **Attack Vector:** Remote (Internet, Wi-Fi, internal LAN)
- **Attack Complexity:** Low to moderate
- **Privileges Required:** None (typical Smart TV services exposed)
- **User Interaction:** Not required
- **Exploitation Status:** Feasible and observed in real-world incidents

4. Affected Systems

The following environments are considered at significant risk:

a. **Smart / Internet-Enabled IPTV devices** connected to the internet or internal networks.
b. Devices deployed in:
   i. Conference and meeting rooms
   ii. Senior leadership offices
   iii. Operations/command centers
   iv. Spaces where classified, restricted, or sensitive deliberations occur
c. Smart TVs with active microphones, cameras, or wireless features.
d. Devices with auto-update enabled or running unverified firmware.
e. IPTV systems connected to unsegmented or flat networks.

5. Exploit Conditions

Successful exploitation may require:

a. Network access to Smart / Internet-Enabled IPTV devices via Wi-Fi, LAN, or internet exposure.
b. Presence of open service ports or vulnerable firmware.
c. Enabled microphones/cameras.
d. Lack of device isolation or segmentation.
e. Absence of enterprise-grade security controls or monitoring.

6. Recommendations & Mitigation Actions

6.1 Immediate Restriction of Smart / Internet-Enabled IPTV Devices

a. Discontinue the Smart / Internet-Enabled IPTV devices in all sensitive areas, including

i. Conference rooms
ii. Command/operations centers
iii. Senior leadership offices
iv. Strategic planning rooms
v. Environments handling classified or operational information

b. Remove internet-connected features and disconnect such devices from internal networks.

6.2 Transition to Secure Alternatives

Organizations must replace banned devices with one of the following:

a. Non-internet-based traditional televisions
b. Hardened, non-Internet IPTV systems, such as the secure isolated IPTV solution developed by NTC, featuring enhanced protections against microphone, camera, and malware-based threats.
c. Prioritize these approved solutions for all sensitive areas.

6.3 Strengthen Device and Network Security Posture

a. Conduct mandatory security assessments before deployment of any audiovisual device.
b. Physically disable or remove microphones and cameras where feasible.
c. Implement strict network segmentation preventing TV devices from accessing sensitive networks.
d. Maintain an asset inventory of all Smart / Internet-Enabled IPTV devices.
e. Allow firmware updates only from trusted sources; disable auto-updates.

f. Monitor network traffic for signs of unauthorized communication or data exfiltration.

7. Monitoring & Detection

Organizations should:

a. Inspect network logs for unusual outbound traffic originating from **Smart / Internet-Enabled IPTV devices**.
b. Monitor for unexpected network scans or lateral movement attempts.
c. Detect unauthorized activation of microphones/cameras.
d. Track anomalies in device OS behavior, firmware updates, or unexplained reboots.
e. Correlate logs in SIEM platforms to identify early indicators of compromise.

8. Incident Response & Readiness

a. Update incident response playbooks to address **Smart / Internet-Enabled IPTV device** compromise scenarios.
b. Immediately isolate any suspected device and collect forensic evidence.
c. Conduct a full sweep of connected networks for signs of associated intrusion.
d. Validate that no meeting data, credentials, or network information was exfiltrated.
e. Ensure verified offline backups of room configuration and device inventory records.

9. Security Status Summary

Category	Device Status	Required Action
Vulnerable	**Smart / Internet-Enabled IPTV devices** in sensitive areas	**Immediate removal or disconnection**
Secure	Non-internet TVs or NTC's hardened non-internet IPTV solution	No additional action required

10. Call to Action

National CERT urges all organizations to:

a. Immediately discontinue Smart / Internet-Enabled IPTV device use in all sensitive environments.
b. Replace these devices with approved non-internet or hardened IPTV solutions.
c. Enforce strict segmentation, monitoring, and security controls.
d. Integrate IoT/Smart device risk assessments into enterprise security governance.

Failure to comply may result in surveillance, data leakage, or compromise of organizational operations.

10. Call to Action

National CERT urges all organizations to:

a. Immediately discontinue Smart / Internet-Enabled IPTV device use in all sensitive environments.
b. Replace these devices with approved non-Internet or hardened IPTV solutions.
c. Enforce strict segmentation, monitoring, and security controls.
d. Integrate IoT/Smart device risk assessments into enterprise security governance.

Failure to comply may result in surveillance, data leakage, or compromise of organizational operations.

Annexure B

CVE Threat Matrix for Smart / Internet-Enabled IPTV Device Risk Context

Threat Category	Description	Relevant CVEs (Examples)	CVSS Score	Attack Vector	User Interaction	Affected Platforms	Impact	Exploit Conditions
Remote surveillance	Covert activation of camera/mic via vulnerable video conferencing clients	CVE-2019-13450 (Zoom macOS forced webcam activation)	6.6 (Medium)	Remote (malicious webpage + app local server)	Required	Zoom macOS legacy versions	Privacy breach, unauthorized audiovisual access	Outdated Zoom client + local web server active
Network filtration	Exploitation of exposed ports and insecure network services to gain internal access	CVE-2021-44228 (Log4Shell RCE), CVE-2020-1472 (Zerologon – domain takeover)	10.0 (Critical)	Remote (direct to open service)	None	Servers, domain controllers, any exposed TCP/UDP service	RCE, lateral movement, full network compromise	Vulnerable service reachable on an open port
Malware Deployment	Installation of malicious software via insecure OS, boot chain, or firmware	CVE-2022-41099 (Secure Boot Bypass), CVE-2021-34481 (Spooler Elevation)	8.8 / 7.8 (High)	Remote or local depending on exploit	Sometimes required	Windows, Linux, macOS, routers, IoT devices	Malware installation, persistence, system takeover	Outdated OS/firmware, weak integrity checks
Data Ailtration	Unauthorized transmission of sensitive data from compromised devices	CVE-2023-23397 (Outlook NTLM leak), CVE-2021-44228 (Log4Shell enabling data theft)	9.8 / 10.0 (Critical)	Remote (via malware, RCE, or compromised apps)	Not required	Any compromised endpoint or server	Theft of documents, credentials, espionage, IP loss	Device already compromised + outbound channel allowed