



Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 189

23-05-2023

Name: Unpatched 5-year-old Vulnerability in TBK DVR Devices Actively Exploited by Hackers

Threat Classification: Authentication Bypass

Affected Services:

- TBK DVR Devices

Summary:

Hackers are exploiting an unpatched five-year-old vulnerability (CVE-2018-9995) in TBK digital video recording (DVR) devices, allowing them to gain administrative privileges and access camera video feeds. Fortinet FortiGuard Labs has warned of over 50,000 attempts to exploit TBK DVR devices using the flaw in April 2023 alone.

Severity	High
Attack Vector	Network

The vulnerability is due to an error when handling a malicious HTTP cookie, and there are currently no fixes that address it.

Recommendations:

- Users of the affected TBK DVR devices should disconnect them from the internet until a patch is available.
- Monitor network traffic and apply network security controls to detect and block malicious traffic targeting the devices.
- Conduct regular VAPT activities to identify and address such security flaws.
- In case of any incident, please report to this office, through PTA CERT Portal and email.