FORTINET

FortiGuard Labs Outbreak Alerts

TBK DVR Authentication Bypass Attack

DVR camera system vulnerability actively exploited in the wild

https://tbkvision.com/
CVEs: CVE-2018-9995

FortiGuard Labs observed "Critical" level of attack attempts to exploit an Authentication Bypass Vulnerability in TBK DVR devices (4104/4216) with upto more than 50,000+ unique IPS detections in the month of April 2023. The 5-year-old vulnerability (CVE-2018-9995) is due to an error when handling a maliciously crafted HTTP cookie. A remote attacker may be able to exploit this flaw to bypass authentication and obtain administrative privileges eventually leading access to camera video feeds.

Background

TBK Vision is a video surveillance company which provides network CCTV devices and other related equipment such as DVRs for the protection of critical infrastructure facilities. According to the vendor website, they have over 600,000 Cameras and 50,000 Recorders installed all over the world in multiple sectors such as Banking, Retail, Government etc. According to the NIST NVD database, TBK DVR4104 and DVR4216 devices are also rebranded and sold as other brands such as Novo, CeNova, QSee, Pulnix, XVR 5 in 1, Securus, Night OWL, DVR Login, HVR Login, and MDVR.

Another notable spike to mention is IPS detections related to MVPower CCTV DVR models (CVE-2016-20016) also known as JAWS webserver RCE. Previously seen to be exploited in the wild through 2017 and on-going. See additional resources for more information.

Latest Developments

FortiGuard Labs is not aware of any patches provided by the vendor and recommends organizations to review installed models of CCTV camera systems and related equipment for vulnerable models.

- December 16, 2024: Federal Bureau of Investigation (FBI) released this Private Industry Notification (PIN) to highlight HatsuRAT scanning campaigns against Chinese-branded web cameras and DVRs.

  HatsuRAT is a Remote Access Trojan (RAT), and according to the report, HatsuRAT actors conducted a scanning campaign targeting Internet of Things (IoT) devices in the US, Australia, Canada, New Zealand, and the United Kingdom.
  https://www.ic3.gov/CSA/2024/241216.pdf
- May 01, 2023: With tens of thousands of TBK DVRs available under different brands, publicly-available PoC code, and an easy-to-exploit makes this vulnerability an easy target for attackers. The recent spike in IPS detections shows that network camera devices remain a popular target for attackers.
- May 10, 2018: Fortinet customers remain protected by the IPS signature to block attack attempts related to vulnerable TBK DVR devices. (CVE-2018-9995)

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Lure

- FortiDeceptor *v3.3+*

Decoy VM

- FortiDeceptor *v3.3+*

AV

Detects known malware related to the Outbreak

- FortiADC *DB 315*
- FortiCASB *DB 315*
- FortiCWP *DB 315*
- FortiClient *DB 315*
- FortiGate *DB 315*
- FortiMail *DB 315*
- FortiProxy *DB 315*
- FortiSASE *DB 315*
- FortiWeb *DB 315*

IPS

Detects and blocks attack attempts leveraging the vulnerability

- FortiADC *DB 13.370*
- FortiGate *DB 13.370*
- FortiNDR *DB 13.370*
- FortiProxy *DB 13.370*
- FortiSASE *DB 13.370*

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

IOC

- FortiAnalyzer
- FortiSOCaaS
- FortiSIEM
- FortiSOAR

Outbreak Detection

- FortiAnalyzer *DB 2.00001*

Threat Hunting

- FortiAnalyzer *v6.4+*
- FortiSIEM *v6.6+*

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automaticlly respond to this outbreak.

- FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

- Incident Response
- FortiRecon: ACI

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

- NSE Training
- Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.

- Security Awareness & Training

InfoSec Services

Security readiness and awareness training for SOC teams, InfoSec and general employees.

- Response Readiness

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

- Security Rating

Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.

- Security Rating

Additional Resources

Hikvision Outbreak Report	https://www.fortiguard.com/outbreak-alert/hikvision-command-injection
CVE-2016-20016	https://www.fortiguard.com/encyclopedia/ips/43737
CVE-2018-9995	https://github.com/vezel/CVE-2018-9995_dvr_credentials
FortiGuard Threat Signal	https://www.fortiguard.com/threat-signal-report/5152

Learn more about FortiGuard Outbreak Alerts

FortiGuard Labs

FORTINET