# 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.

**Announced**

May 10, 2018: Fortinet customers remain protected by the IPS signature to block attack attempts related to vulnerable TBK DVR devices. (CVE-2018-9995)

**Latest Developments**

May 1, 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.

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.

# PROTECT

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

### Reconnaissance

#### Lure

FortiDeceptor
*v3.3+*

#### Decoy VM

FortiDeceptor
*v3.3+*

### Weaponization

### Delivery

### Exploitation

#### IPS

**Detects and blocks DVR Cookie Authentication Bypass Attack (CVE-2018-9995)**

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

### Installation

### C2

### Action

# DETECT

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

#### Outbreak Detection

FortiAnalyzer
*DB 2.00001*

#### Threat Hunting

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

#### Content Update

FortiSIEM
*DB 315*

# RESPOND

**Develop containment techniques to mitigate impacts of security events:**

#### Automated Response

**Services that can automatically 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:**

#### 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 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 | FortiRecon: EASM |
|---|---|

# 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/eezeit/CVE-2018-9995_dvr_credentials |
| **FortiGuard Threat Signal** | https://www.fortiguard.com/threat-signal-report/5152 |

Learn more about FortiGuard Outbreak Alerts