



Multiple Vendor Camera System Attack

Active attack attempts targeting vulnerable CCTV Cameras and DVR systems from multiple vendors such as Argus, Axis, MVPower and Vacon.

CVEs: CVE-2018-15745, CVE-2018-10661, CVE-2018-10662, CVE-2016-20016

FortiGuard Labs observed actively targeted video surveillance systems which may be without any available patches. Some of the attack attempts were peaked to as much as 50,000 IPS devices in the month of April 2023.

Background Recently, FortiGuard Labs released an Outbreak Alert on TBK DVR systems which had critical level of attack attempts based on our IPS telemetry. We expanded our research on such attacks and have discovered other devices that are being actively targeted and may be without any vendor patch.

- Announced**
1. CVE-2018-15745: Argus Surveillance DVR 4.0.0.0 Devices- The flaw allows Unauthenticated Directory Traversal leading to file disclosure.
 2. CVE-2018-10661 and CVE-2018-10662: Multiple models of Axis IP Cameras- This flaw allows for bypass of Access Control and exposed Insecure Interface which attacker may exploit to gain system access.
 3. CVE-2016-20016: MVPower CCTV DVR Models- A remote unauthenticated attacker can execute arbitrary operating system commands as root. This vulnerability has also been referred to as the "JAWS webservice RCE"
 4. Vacon NVR Remote Code Execution- Attack against a Command Injection vulnerability in VACRON Network Video Recorder. This vulnerability does not have any assigned CVE yet.
 5. Beward N100 Remote Command Execution- A Command Injection vulnerability in Beward N100 H.264 VGA IP Camera. This vulnerability does not have any assigned CVE yet.

Latest Developments The active exploitation attempts of these surveillance systems mentioned are already protected by IPS signatures and Fortinet customers remain protected from such attacks. FortiGuard Labs further recommends organizations to review affected vendor models and review for any vendor patches where possible.

PROTECT

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

- Reconnaissance**
 - Decoy VM**

Detects and blocks attack attempts related to multiple vendor camera system attack and prevents lateral movement on the network segment

FortiDeceptor
v3.3+
- Weaponization**
- Delivery**
- Exploitation**
 - IPS**

Detects and blocks attack attempts related to multiple vendor camera system attack

FortiGate DB 15.867

FortiSASE DB 15.867

FortiNDR DB 15.867

FortiADC DB 15.867

FortiProxy DB 15.867
- 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 2.00004
- Threat Hunting**

FortiAnalyzer v6.4+

FortiSIEM v6.4+
- Content Update**

FortiSIEM
DB 316

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

- Axis Affected Product List https://www.axis.com/files/sales/ACV-128401_Affected_Product_List.pdf
- TBK DVR- Outbreak Alert <https://www.fortiguard.com/outbreak-alert/tbk-dvr-attack>
- Hikvision IP Cameras- Outbreak Alert <https://www.fortiguard.com/outbreak-alert/hikvision-command-injection>

Learn more about [FortiGuard Outbreak Alerts](#)