OUTBREAK ALERTS



Multiple Vendor Camera System Attack

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

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 webserver RCE" 4. Vacron 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

Reconnaissance

Decoy VM

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



Weaponization

Delivery

Exploitation

IPS

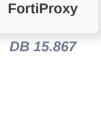
Detects and blocks attack attempts related to multiple vendor camera system attack











C2 Action

Installation

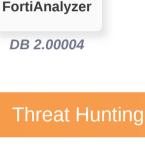


Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

DETECT

Outbreak Detection









FortiSIEM

v6.4+



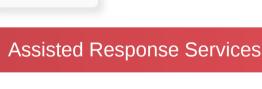


Automated Response

RESPOND

Services that can automaticlly respond to this outbreak.

Develop containment techniques to mitigate impacts of security events:



FortiXDR

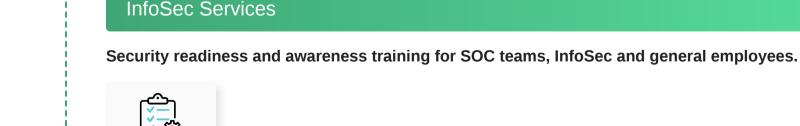
Experts to assist you with analysis, containment and response activities.

Incident FortiRecon: Response





(and recovery from) security incidents:





Response Readiness



IDENTIFY

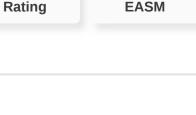
Security reconnaissance and penetration testing services, covering both internal & external attack vectors,

Identify processes and assets that need protection:





Security



Additional Resources Axis Affected Product List

TBK DVR- Outbreak Alert

https://www.axis.com/files/sales/ACV-128401 Affected Product List.pdf https://www.fortiguard.com/outbreak-alert/tbk-dvr-attack

Alert

FEBRINET

Learn more about FortiGuard Outbreak Alerts