مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Mirai Botnet Exploits Zero-Day Vulnerability in AVTECH IP Cameras

Tracking #:432316205
Date:30-08-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a widespread Mirai botnet campaign exploiting a recently disclosed zero-day vulnerability in AVTECH IP cameras.

TECHNICAL DETAILS:

A widespread Mirai botnet campaign exploiting a recently disclosed zero-day vulnerability (**CVE-2024-7029**) in AVTECH IP cameras. The vulnerability, which allows for remote code execution, has been leveraged to propagate a Mirai variant dubbed "Corona," raising significant concerns about critical infrastructure security.

Vulnerability Details:

- **CVE-2024-7029 |** Base Score: 8.8 | Severity: High | COMMAND INJECTION
  - A Remote Code Execution (RCE) vulnerability found in the "brightness" function of AVTECH IP cameras.
  - This flaw allows malicious actors to execute command injections remotely, granting them elevated privileges on the target system.
  - Exploiting this vulnerability, attackers can deploy a variant of the notorious Mirai botnet, spreading malware with alarming efficiency.
  - A proof of concept (PoC) for CVE-2024-7029 publicly available

Affected Versions: AVM1203: firmware version FullImg-1023-1007-1011-1009 and prior

Mitigation: While a patch for CVE-2024-7029 is not yet available, it is recommended to decommission affected devices as the most effective mitigation strategy.

Note: It is also observed that attackers are also targeting several other vulnerabilities, including those in AVTECH devices, a Hadoop YARN RCE, CVE-2014-8361, and CVE-2017-17215.

RECOMMENDATIONS:

- **Decommission Affected Devices:** The most effective mitigation is to decommission AVTECH IP cameras that are vulnerable to CVE-2024-7029.
- **Network Segmentation:** Isolate affected devices from critical networks to limit the potential impact of a successful attack.
- **Intrusion Detection Systems (IDS):** Deploy IDS solutions to monitor network traffic for suspicious activity and detect potential attacks.
- **Regular Updates:** Ensure that all other devices and systems are kept up-to-date with the latest security patches and updates.
- **Security Awareness Training:** Educate staff about the risks associated with this vulnerability and the importance of following best practices for cybersecurity.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.akamai.com/blog/security-research/2024/aug/2024-corona-mirai-botnet-infects-zero-day-sirt