CVE-2021-29255 Vulnerability Disclosure

Overview: Below is vulnerabilities discovered in IP cameras produced by MicroSeven. These vulnerabilities may apply to additional Camera models and firmware versions than listed herein. This report discloses two different vulnerabilities.

Vulnerability: Unencrypted Transmission of Admin Credentials.

Summary: Unencrypted Transmission of Admin Credentials for Web Management interface in MicroSeven's IPCamera model MYM71080i-B affecting firmware versions v2.0.5 to v2.0.20. Allows an unauthenticated attacker on the local network to gain admin credentials to the IPCamera's web interface.

MicroSeven's IPCamera model MYM71080i-B calls back to MicroSeven's Cloud Services (pnp.microseven.com:7007) in an unencrypted TCP session. The session contains the administrative username and password in cleartext.

Product: MYM71080i-B

Product App Version: Confirmed in version F2.0.05 to F2.0.20

Steps to reproduce:

1. Install a network capture method(software or hardware-based) between the IPCamera and the IPCamera's connection to the Internet.
2. Wait for the IPCamera to call out to IP 173.254.193.108(AKA: pnp.microseven.com) on port 7007. This call occurs in roughly 30-minute intervals.
3. Within the captured network traffic will contain the following cleartext exchange of strings.

TO-173.254.193.108 FROM-IPCamera

"554|80|2048|2048|512|admin|password|MYM71080i-B-F2.0.11"

Response-FROM-173.254.193.108 TO-IPCamera

"……………30"

Final-Response-TO-173.254.193.108 FROM-IPCamera

"…………R…1083D2000E0B0000"

Impact: An attacker on the same network as the IPCamera can gain admin access to the device. The attacker can achieve a network traffic capture using trivial man-in-the-middle attack techniques, such as ARP Poisoning. This admin access can give an attacker the ability to update the firmware with a malicious firmware package, giving an attacker persistent access in a network.

Recommendation:

Encrypt the communications between IPCamera and outbound calls to MicroSeven Systems using SSL/TLS.

Vulnerability: Unauthenticated firmware version disclosure

Summary: An unauthenticated remote attacker can discover the IPCamera's currently running firmware version by opening a link to the web interface.

Product: MYM71080i-B

Product App Version: Confirmed in version F2.0.04 to F2.0.25

Steps to reproduce:

1. Open the URL "http://192.168.10.201/web.ini". Replace the IP 192.168.10.201 with the IPCamera's current IP.

Result

____

[vercfg]

webver = “v2.0.11 “
m7ver = “MYM71080i-B-F2.0.11”
——————————————

Impact: An attacker can learn the IPCamera’s current firmware version. This information can be used to find known vulnerabilities, or download the firmware version online and discover new vulnerabilities to exploit.

Recommendation:

Require user authentication before allowing access to read the “web.ini” file.

Recommended Reading: Lab – Exploiting CVE-2021-29255

Post Views: 127

Related Posts:

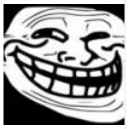
Lab: Exploiting CVE-2021-29255

Lab: Breaking Guest WiFi

Bypass 2FA on Windows Servers

Getting My Certified Ethical

Home Network Security TAP

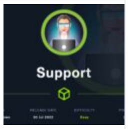


Gray Hatting Spam: I did it for

Red Team Tools: Reverse Shell

Webserver VHosts Brute-

RedTeam Tip: Hiding Cronjobs



HTB Walkthrough:

Bret

I'm an IT Professional with more than a decade in the IT industry. My security skills were built on years of strong systems administration work, and practice.
My motto is, "If you're not pushing forward, your falling behind!"

Certs: EC-Council Certified Ethical Hacker, MS MCSA: Windows Server 2016, CompTIA Net+
Follow me on Mastodon

March 26, 2021

Red Team, Security Research

CVE-2021-29255, Network Security, Red Team, Vulnerability Disclosure

Previous post

Next post

0 Comments

8 Pingbacks

Vulnerability Summary for the Week of March 22, 2021 – 1stCyberSecurity.Com

Vulnerability Summary for the Week of March 22, 2021 - Taurus Technology

Vulnerability Summary for the Week of March 22, 2021 | Smart Cyber Security

Vulnerability Summary for the Week of March 22, 2021 | Som2ny Network

Vulnerability Summary for the Week of March 29, 2021 | MacTech.com

Vulnerability Summary for the Week of March 29, 2021 - Taurus Technology

Lab: Exploiting CVE-2021-29255 - Cyber Gladius

Vulnerabilidad en () - CVE-2021-29255 - Información y Soluciones

COMMENTS ARE CLOSED.

UP ↑