CVE-2021-33820

[Discoverer]

*Jian Xian Li, *Hao Hsiang Lin, Guan Yu Lai

Telecom Technology Center

(TTC is an experienced cybersecurity professional team. It helps companies to improve their security posture, and increase the confidence in implementing, and assessing the right security controls and vulnerabilities of network-connectable consumer/medical/industrial products.)

[Description]

An issue was discovered in UniFi Protect G3 FLEX Camera Version UVC.v4.30.0.67. Attacker could send a huge amount of TCP SYN packet to make web service's resource exhausted. Then the web server is denial-of-service.

[Attack Type]

Remote

[Product]

UniFi Protect G3 FLEX Camera

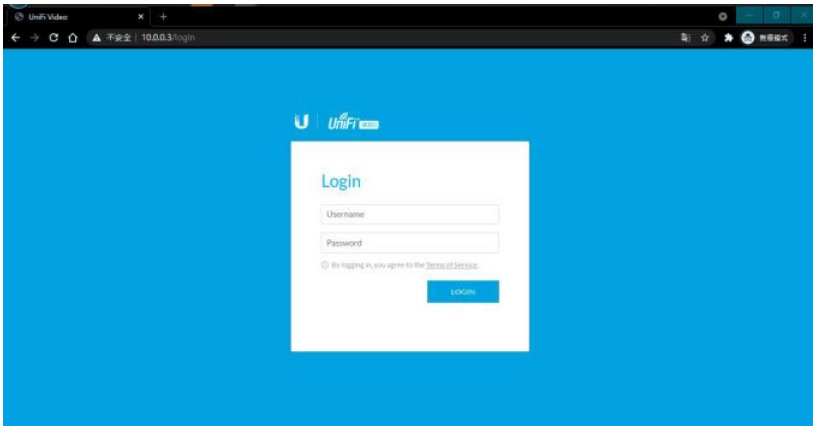
[Version]

UVC.v4.30.0.67

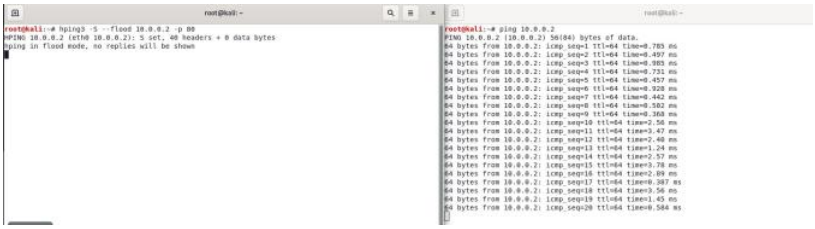
UniFi Protect G3 FLEX Camera devices vulnerability

Demonstration

Normally, UniFi Protect G3 FLEX Camera's web login screenshot is like this. As shown below:

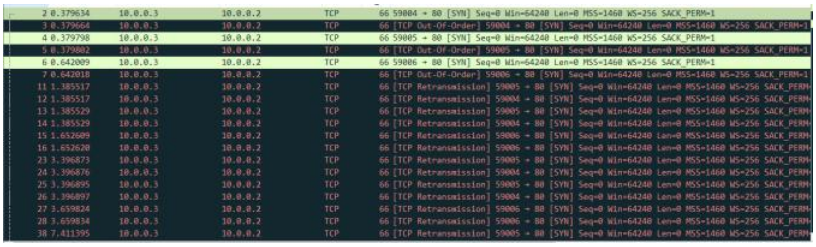


By using hping3 tool to attack to UniFi Protect G3 FLEX Camera's web server, through send SYN packets repeatedly. Making UniFi Protect G3 FLEX Camera's web services' resource exhausted. If attack cause web server out of service successfully. As shown below:



It makes clients unable to access the web service when the attack was successful As shown below:

It could be found on wireshark by capturing packets that web service will not be able to provide service normally when client send request to UniFi Protect G3 FLEX Camera As shown below:



Reference(s)

https://linuxhint.com/hping3/

https://store.ui.com/collections/unifi-protect-cameras/products/unifi-video-g3-flex-camera