FAQs: Command Injection Vulnerability

Q: What is the Command Injection Vulnerability?

A: As stated in Hikvision official HSRC-202109-01 Security Notification, a Command Injection Vulnerability was found in the web server of some Hikvision products. Due to an insufficient input validation, an attacker could potentially exploit the vulnerability to launch a command injection attack by sending a specially crafted message with malicious commands.

Q: Where can I get more information?

A:
- Hikvision Security Notification . The company has released Security Notification on the company's website on September 18th and posted on social media accounts on September 19th.
- Security Researcher Disclosure Report

Q: Is this a Chinese government back door?

A: No. Hikvision does not have government backdoors in our products. Watchful_IP, the security researcher who responsibly reported this vulnerability to Hikvision, stated, "No, definitely NOT. You wouldn't do it like this. And not all firmware types are affected."

Q: What has Hikvision done to deal with the vulnerability?

A: Hikvision follows responsible disclosure principles and the standard Coordinated Vulnerability Disclosure Process that is widely accepted in global industries and pertains to the mechanisms by which vulnerabilities are shared and disclosed in a controlled way to best protects the owners and end users of software.

On June 23, 2021, Hikvision was contacted by a security researcher, named Watchful IP, who reported a potential vulnerability in a Hikvision camera. Once we confirmed receipt of this report, Hikvision worked directly with the researcher to patch and verify the successful mitigation of the reported vulnerability.

As the researcher noted in his disclosure report that he was "pleased to note this problem was fixed in the way recommended."

After the company and the researcher both ensured that the vulnerability had properly patched by the updated firmware, we released the Security Notification on the company's website and social media on September 19th.

Q: What's the company's recommendation regarding 'port forwarding'?

A: An industry blog included the misleading information regarding the company's recommendation on 'port forwarding' in its recent post. Please note, according to the company's guideline "About Port Forwarding", Hikvision cautions its end users against port forwarding, and advises that "port forwarding should only be configured when absolutely necessary."

Where end users affirmatively choose to configure port forwarding for devices that need to be accessed via the Internet, Hikvision supports the following cybersecurity best practices: (1) "minimize the port numbers exposed to the Internet," (2) "avoid common ports and reconfigure them to customized ports"; and "enable IP filtering.", （3）Set a strong password, and (4) upgrade to the latest device firmware released by Hikvision in a timely manner.

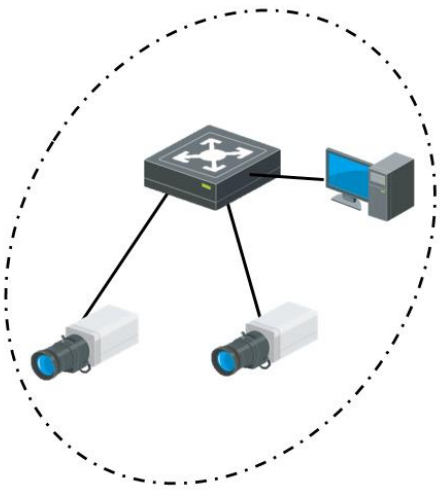
Q: How to evaluate the risks of my Hikvision devices?

A: To exploit this vulnerability, an attacker must be on the same network as the vulnerable device. In other words, if the attacker is able to view the log in screen of a vulnerable device, they could attack it. If they cannot get to the login screen of a vulnerable device, they are not able to exploit the vulnerability.

To evaluate the risk level of a vulnerable device, check if the affected model exposes its http/https servers (typically 80/443) directly to the Internet (WAN), which would give a potential attacker the ability to attack that device from the Internet. Below are some examples:

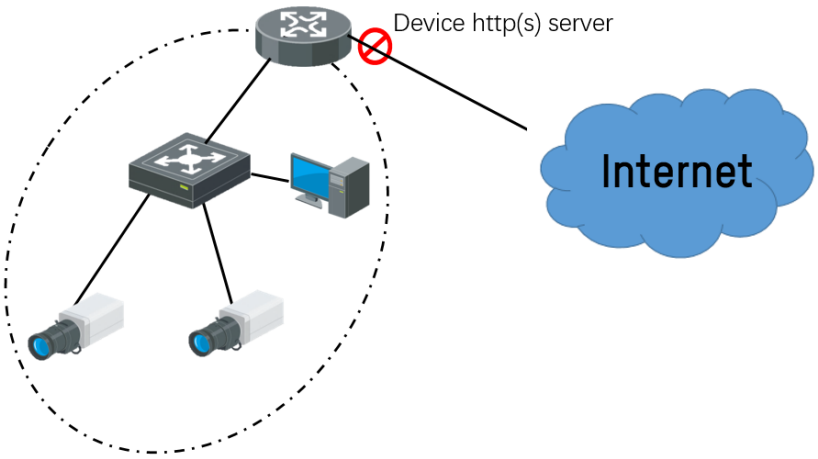
① LAN network without Internet access (low risk)

A potential attacker cannot access the device's web server from the Internet so the risk is low (attacker must have LAN access to exploit this vulnerability, that's what we mean with low risk)



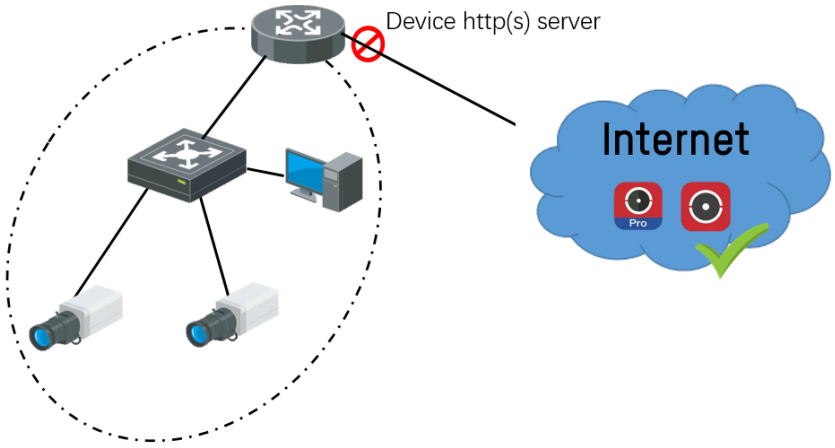
②WAN network with firewall blocking device http(s) server (low risk)

Since the potential attacker still cannot access device web from Internet， in this situation the system is still considered low risk



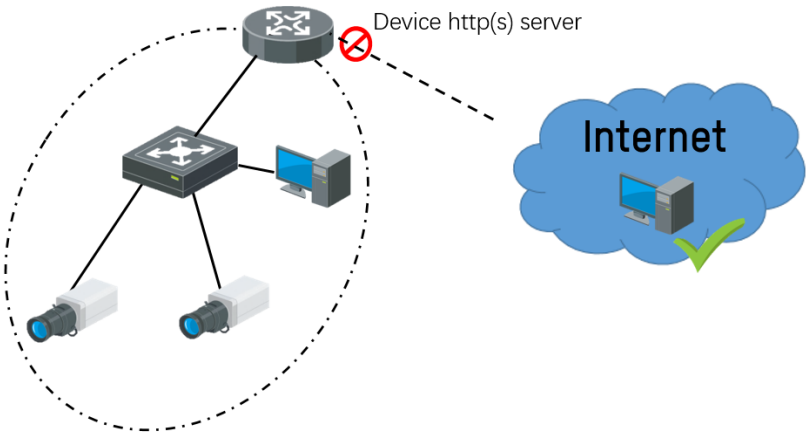
③Hik-Connect & Hik-ProConnect (low risk)

HC and HPC are special cases of the above second scenario, http(s) is not needed in HC/HPC service so it will be as safe as usual



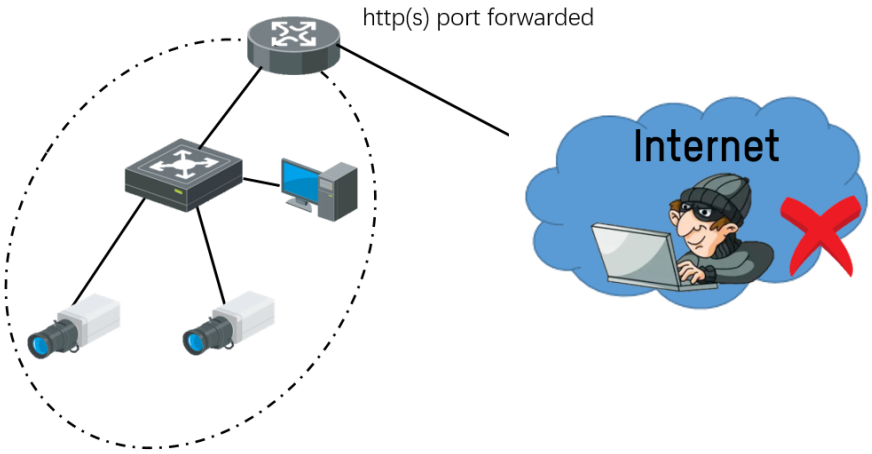
④VPN access from Internet (low risk)

VPN (Virtual Private Network) allows only verified users to login and access devices from site network, so it's a secured way to access device and not easy to be attacked



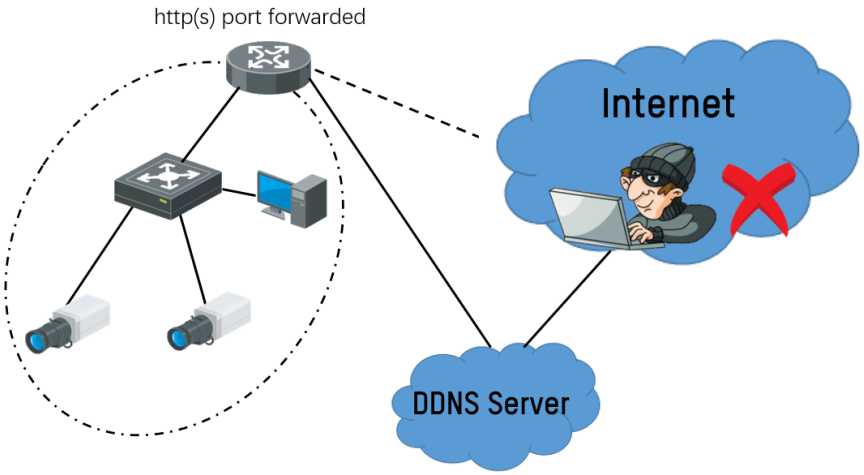
⑤Port forwarding (High Risk)

Port forwarding is an easy and inexpensive way for users to remotely access a device, however port forwarding brings additional risks because it tells the firewall not to block traffic to that device from the Internet on certain ports. Therefore, with the current vulnerability, as long as a potential attacker has access to a device through its forwarded http(s) ports, the device is at high risk of being attacked.



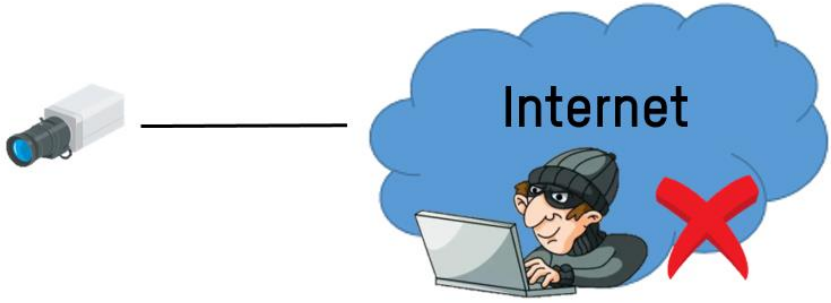
⑥ DDNS (High Risk)

Dynamic DNS (DDNS) also uses port forwarding so a potential attacker could still have access to a device from the Internet, putting the device at high risk of being attacked.



⑦ Direct WAN Access (High Risk)

Some sites install devices directly to Internet (WAN). As long as the device has an open IP address and its http(s) ports are exposed to Internet, the device is at high risk of being attacked.



In brief conclusion, the easiest way to evaluate system risk level is to check if you can access device webpage directly without any extra network variation. If yes, the system should be considered at high risk.

As far as we know, the only people who know how to exploit this vulnerability are the researcher and Hikvision's Security Response Centre. However, now that the patch has been released and attackers know that this vulnerability exists, they will be searching for it. If you have an affected camera/NVR whose http(s) service is directly exposed to the Internet, Hikvision highly recommends you to patch your device immediately (recommended), and using a more secure solution, like a VPN.

NOTE: This document addresses the risk of Internet attack. It assumes that your internal network is properly segmented and that a threat actor has not gained access to your internal network. To further assess risk, determine if your internal network is trusted and if not, take the proper measures to patch and segment your video surveillance network from other parts of your internal network.