HIKVISION®

14th June 2023
Dear Valued Partner,

We have discovered and determined that certain Hikvision NVRs and DVRs may be impacted by a scripted application.

“When the UPnP/NAT feature is enabled and the ports are open, the hacker scans the router to find the IP addresses/ports and then tries brute force attacks utilising generic passwords in an attempt to log into the device”

By accessing the camera or NVR/DVR web page they then over right the OSD Text Overlay and display the message :

> *“Your CCTV is vulnerable and can be exposed,*
> *Fix it pls – DIY or Telegram me – faxociety”*

The devices may be affected if:

- Weak passwords that contain only letters and numbers are used
- They are exposed directly on the open Internet when UPnP/NAT feature is enabled or Port forwarding using default port settings;

We recommend that actions be taken to mitigate potential risks. Please ensure the following hardening practices are employed to provide additional resilience for your customers.

1. As always, password strength is critical. Ensure your customers set up complex passwords containing letters (uppercase and lowercase), numbers, and special characters.
2. Please avoid using the same password multiple times when deploying security systems.
3. In general, we recommend that you disable the UPNP/NAT feature on devices, this will not affect communication with the Hik-Connect server.

In order to delete the text overlay access the devices via your browser, navigate to the menu configuration, image, OSD setting, and then delete the texts. Please then take the above preventative actions.

If you require assistance, don't hesitate to contact Hikvision Support - 1300976305 or email techsupportau@hikvision.com.