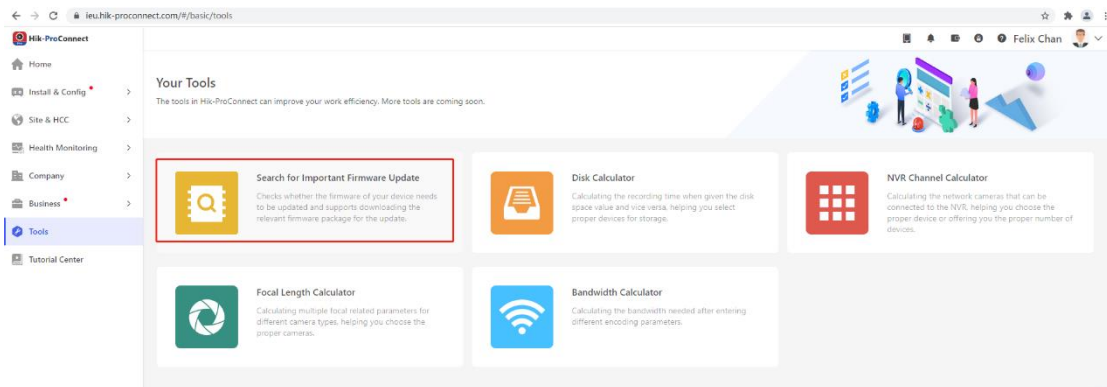


How to Use Search Tool for Important Firmware Update on Hik-ProConnect Portal

- Applicable to Hik-ProConnect V1.9

1. Open *Tools*->*Search for Important Firmware Update*



2. Currently, there are two ways to search for the device affected by security vulnerabilities.

- After opening the tool, it will automatically search in the same LAN.

After searching, you can see the model, serial number, firmware version, IP, port and other information of the vulnerable device.

Search for Firmware

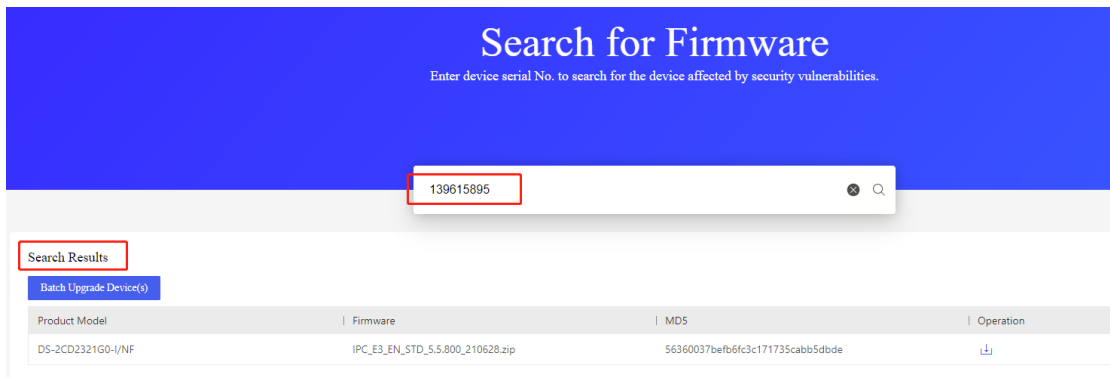
Enter device serial No. to search for the device affected by security vulnerabilities.

Affected Devices on the Same LAN Found by the Tool

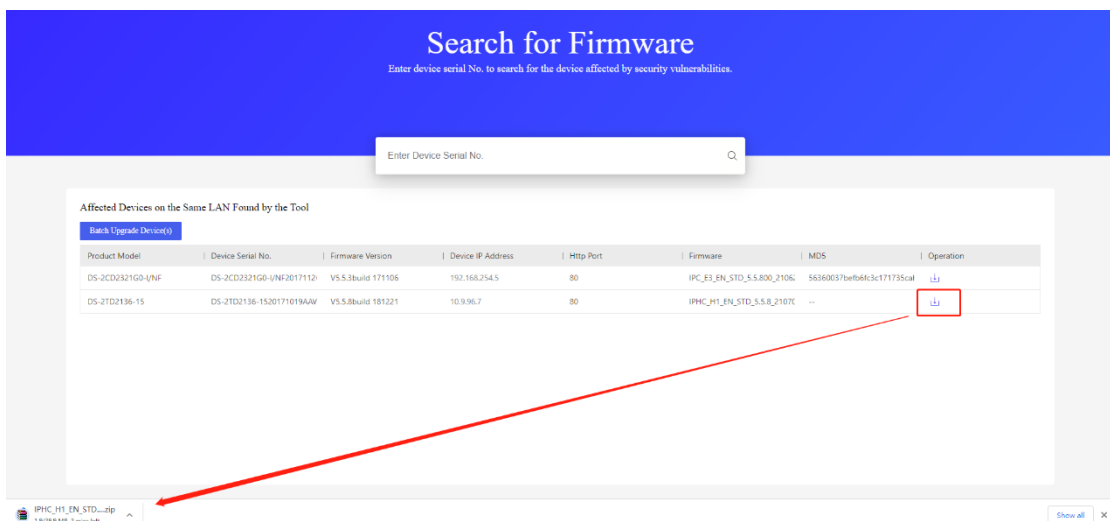
Batch Upgrade Device(s)

Product Model	Device Serial No.	Firmware Version	Device IP Address	Http Port	Firmware	MDS	Operation
DS-2CD2321GD-I/NF	DS-2CD2321GD-I/NF2017112	V5.5.3build 171106	192.168.254.5	80	IPC_E3_EN_STD_5.5.800_2106	56360037befb6fc3c171735cal	↓
DS-2TD2136-15	DS-2TD2136-1520171019AAW	V5.5.8build 181221	10.9.96.7	80	IPHC_H1_EN_STD_5.5.8_2107C	--	↓

- Enter device serial No. manually to search.

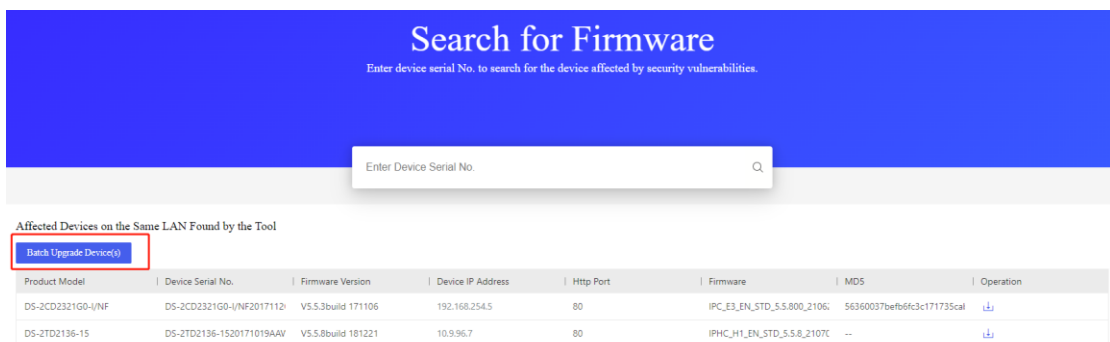


3. Download the secure firmware package and upgrade.



4. Batch upgrade devices


Click *Batch Upgrade Device(s)*, it will jump to the *On-Site Batch Update* page and can be upgraded in batch.

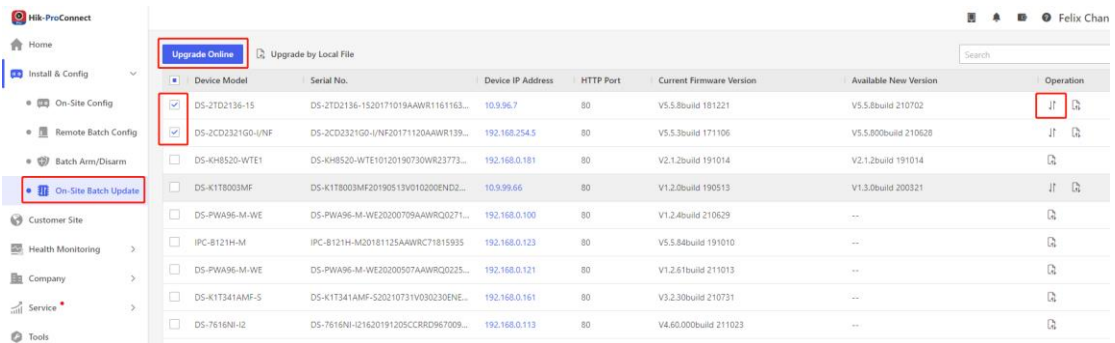


5. On-Site Batch Update


There are two ways to update your devices:

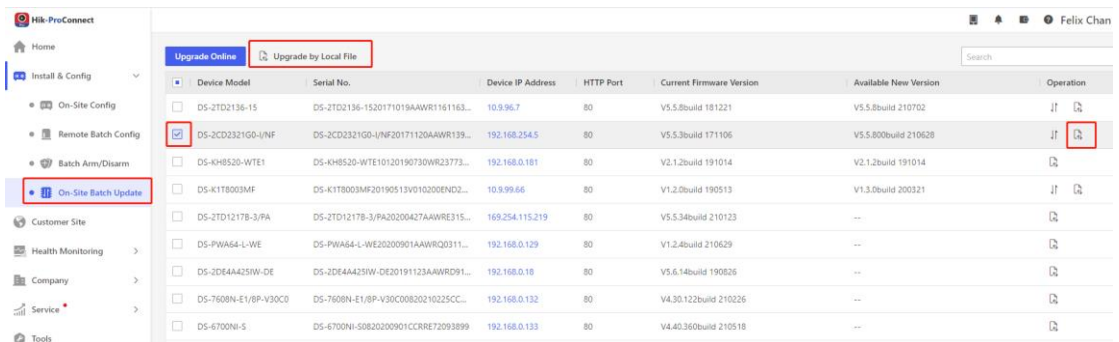
a. Upgrade Online

You can select multiple devices for batch online upgrade, or click  to upgrade a single device. (There is no need to download firmware locally)



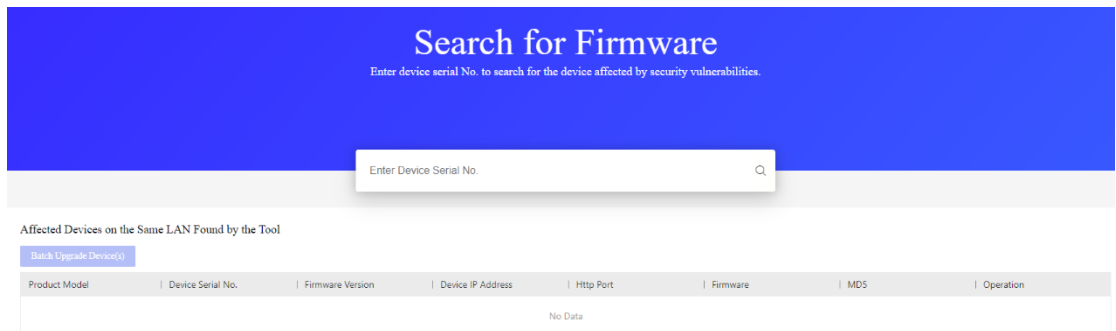
b. Upgrade by Local File

You can check multiple devices of the same model for batch upgrade by local file, or click  to upgrade a single device.

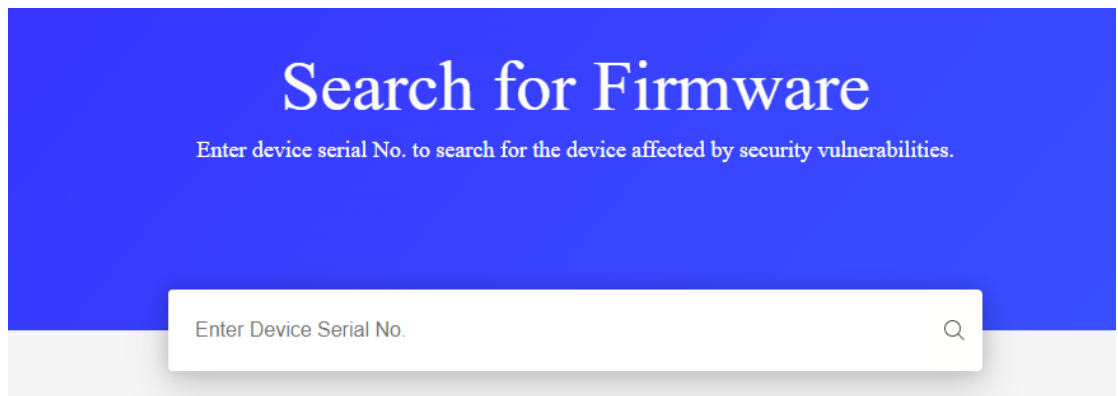


6. Optional

a. If there are no devices to be upgraded in the same LAN where the PC is located, *No Data* will be prompted.



- b. If a device under the network is detected to have the vulnerability, but there is no security upgrade package. There will be the following prompt.



Please contact your Technical Support Team to get the firmware of this serial number.
Only the products whose firmware has security vulnerabilities can be found on the page.