Hikvision Makes Child Pornography Distribution Harder With Improvements To Hik-Connect App

Published on Aug 31, 2023

Generated for Charles Rollet on Aug 02, 2024 for Your Use Only - No Sharing - No Promotions

IPVM recently exposed Child Pornography On Sale From Hacked Hivision Cameras Using Current Hik-Connect App. Now, Hikvison has released a new Hik-Connect app version that makes it harder to do so.

In this report, we examine what the changes are, how this makes it harder, what risks remain, and our recommendations for improvement.

Executive Summary

The changes Hikvision quietly made to Hik-Connect will not stop accounts from being shared with unauthorized access, and a large amount of Hikvision users

will never see the sharing notifications recently implemented.

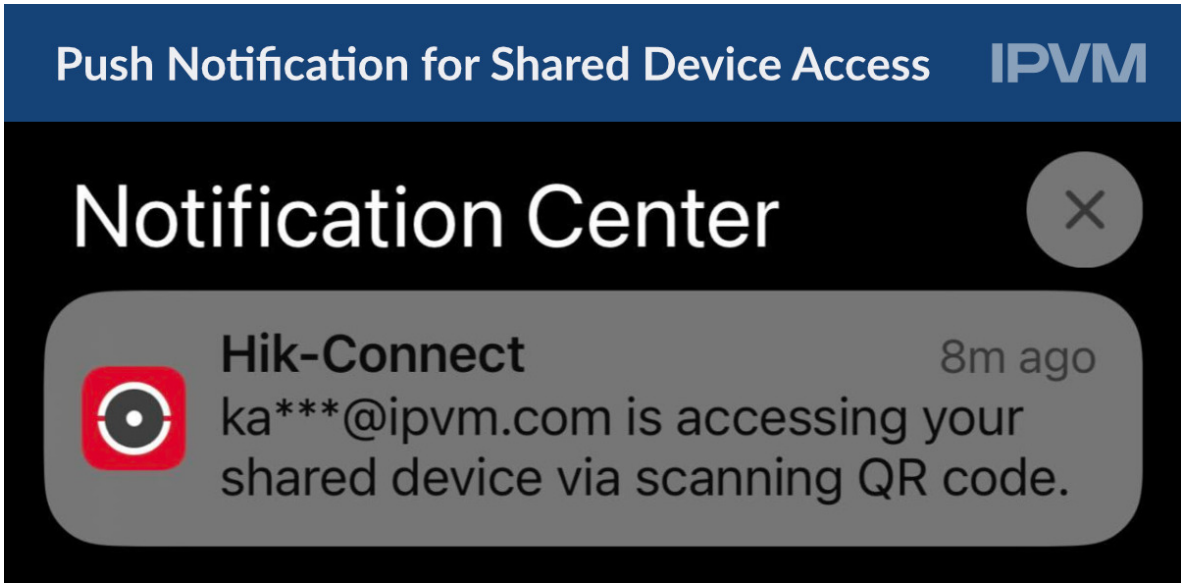
Summary Of Changes

Hikvision made several changes to the way that sharing works within Hik-Connect. Restrictions were added to the number of people that can be shared with, the duration of the share, and also added notifications. The key changes are listed below:

- Shared viewing app notifications are now sent to the Hik-Connect account owner.
- Reduced shared duration to 30 days from 365 days.
- Reduced shared recipients limit to 10 from 50.
- Encryption password is required for shared Hik-Connect viewers.
- Encryption passwords are not required for direct access devices.

Push Notifications Added, Still May Not Be Seen

Hikvision has enabled sharing notifications for the account owner, as shown below:

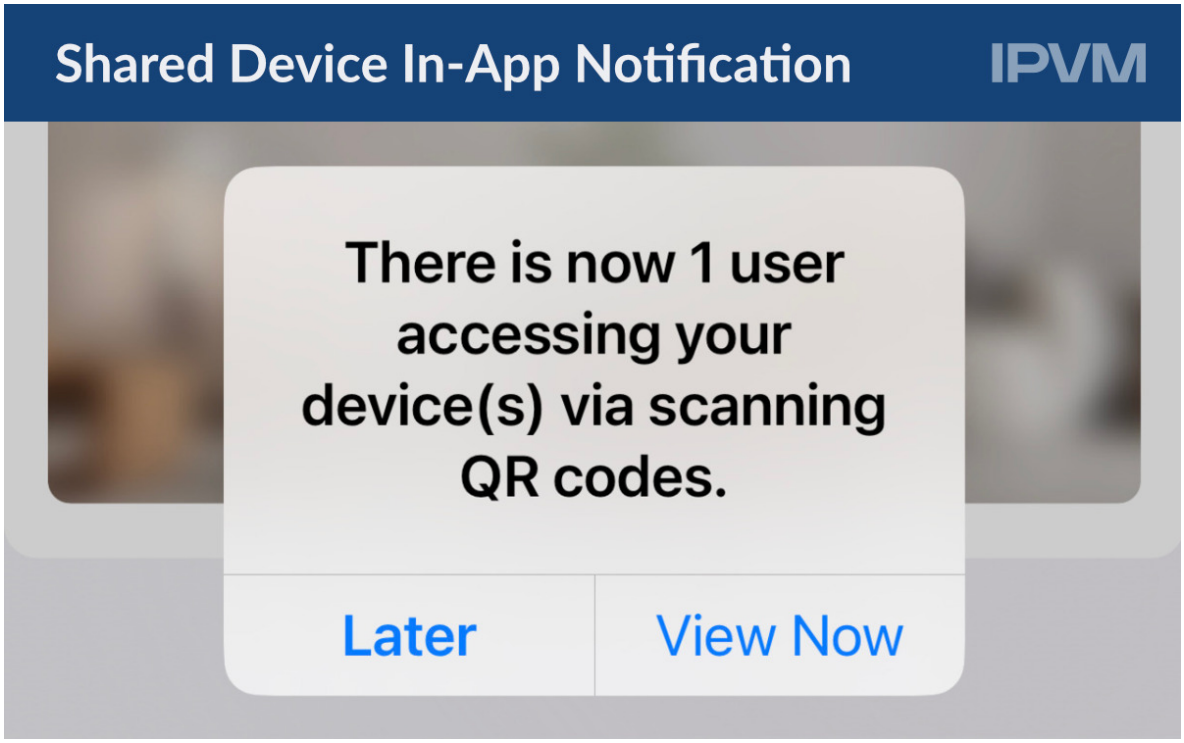


Adding Push notifications was a solid improvement. However, it will have a limited impact. There are several assumptions and problems with the effectiveness of this. This device owner has to have Hik-Connect setup, initially granted permission for notifications, and have not turned off app/push notifications.

Anyone not using Hik-connect will not receive these notifications. Another possible failure is that others may have the app installed and initially enabled notifications but then became frustrated by nuisance alerts and disabled notifications.

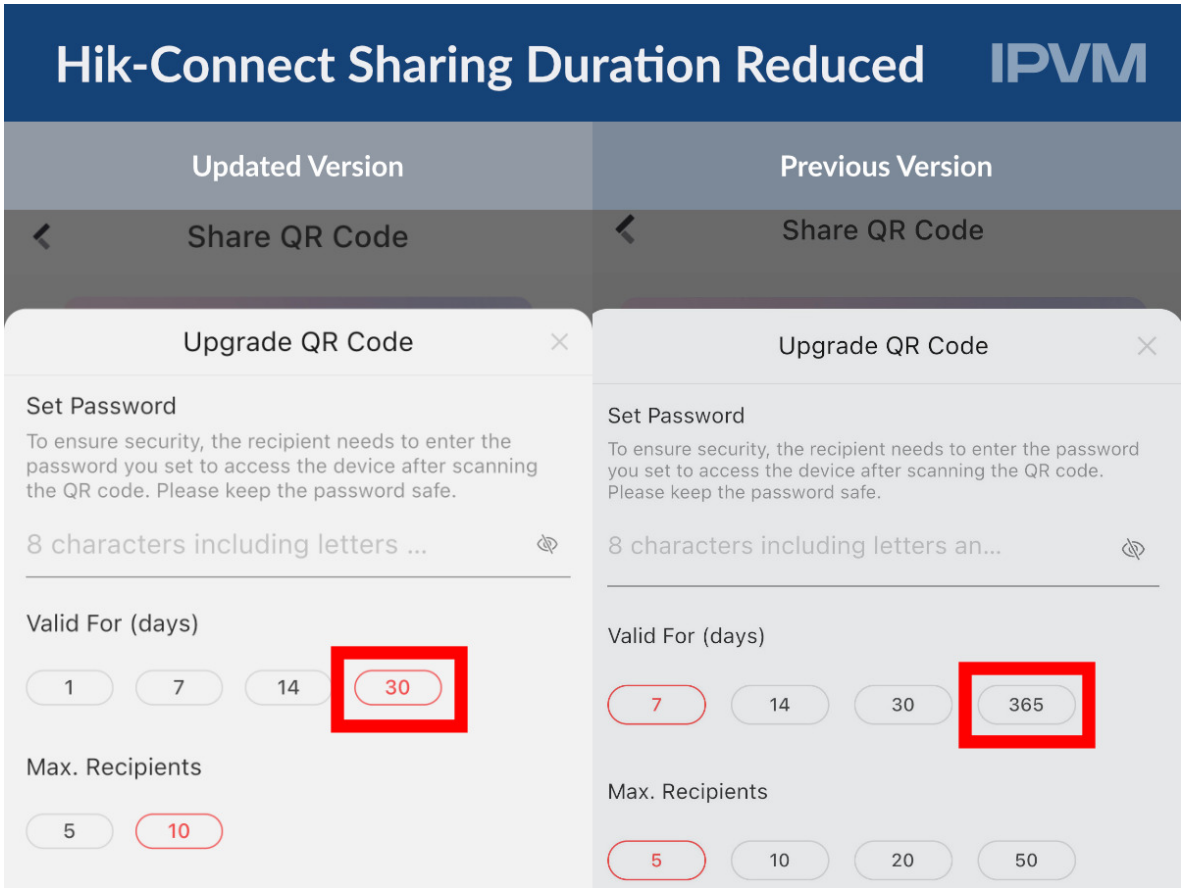
Moreover, Hik-Connect / Platform Access does not need to be enabled on the camera for it to be viewed within the Hik-Connect app, as devices can be directly added via their IP addresses.

If a user does have Hik-Connect setup but notifications disabled, they will not receive push notifications, but they will see an in-app sharing notification if/when they open the app:



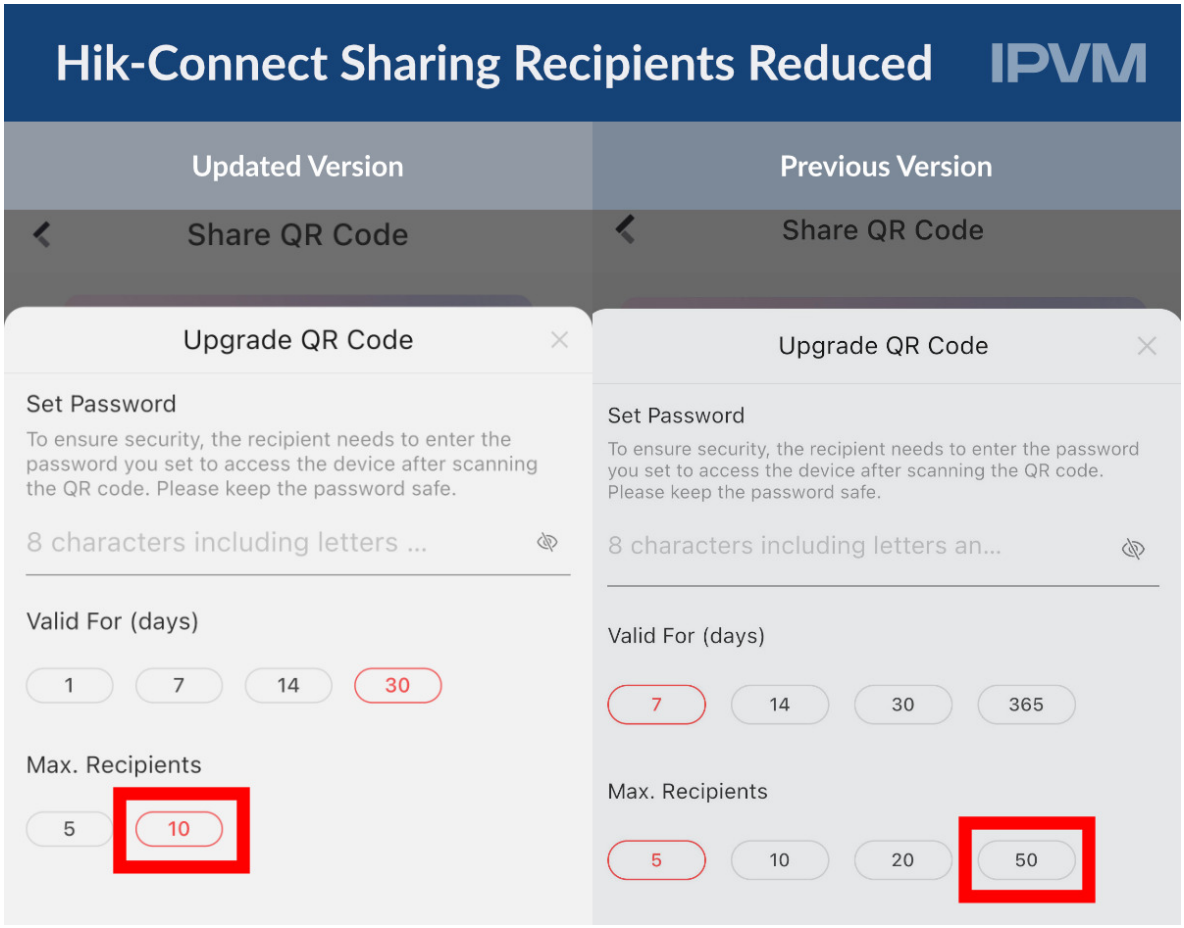
Reduced Share Time to 30 Days

The original sharing duration was 365 days. Hikvision has now limited this to 30 days.



Reduced Shared Recipients Limit to 10

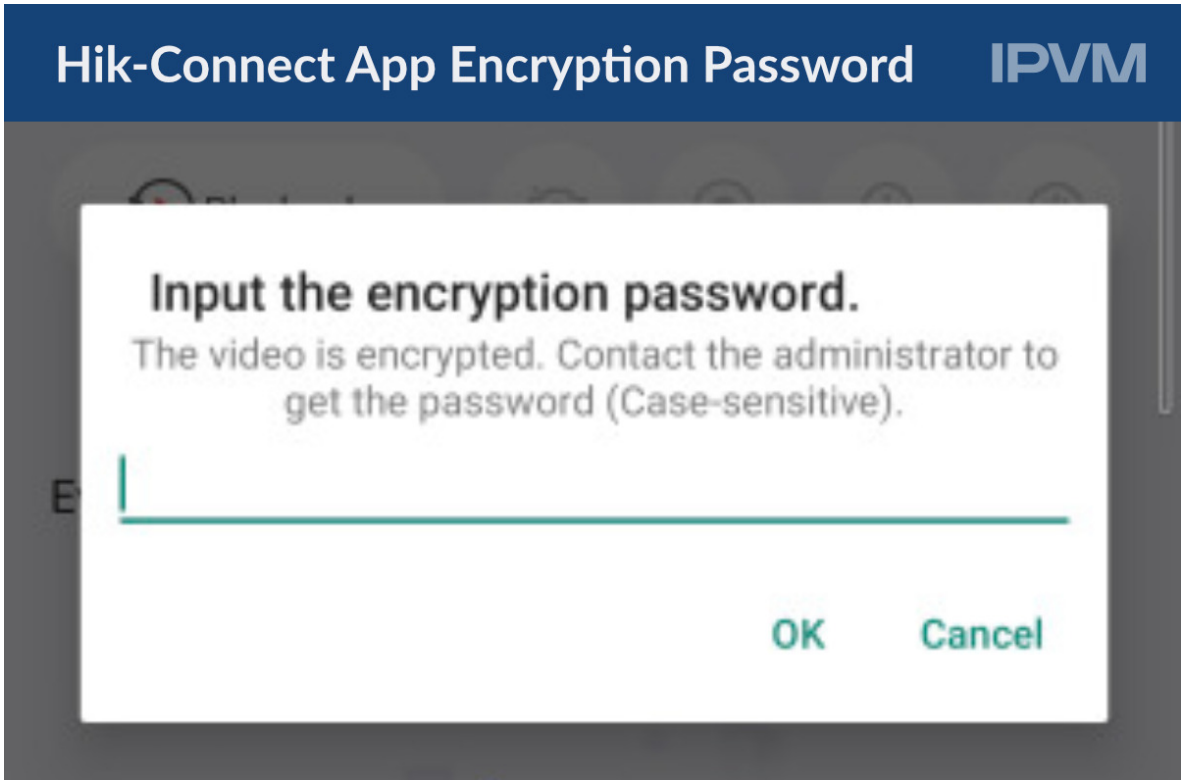
The maximum number of recipients has also been reduced to 10 users per QR code from 50 recipients. This will help prevent multiple resales of a single QR code persisting for many to use. However, there is still no limit on the number of QR codes sharable from a single device.



Encryption Password

Depending on the method used to add the camera, an encryption password may or may not be needed. The encryption password is required for shared Hik-Connect viewers. However, the encryption passwords are not required for direct access devices / devices added via IP address.

When the Hik-Connect cloud camera is shared with other users, the recipient is now required to know the video encryption password before they can see the video feed.



The password is set in the IP camera when the camera is activated for the first Hik-Connect cloud connection and can be changed from the Hik-Connect app if the previous encryption password is known.

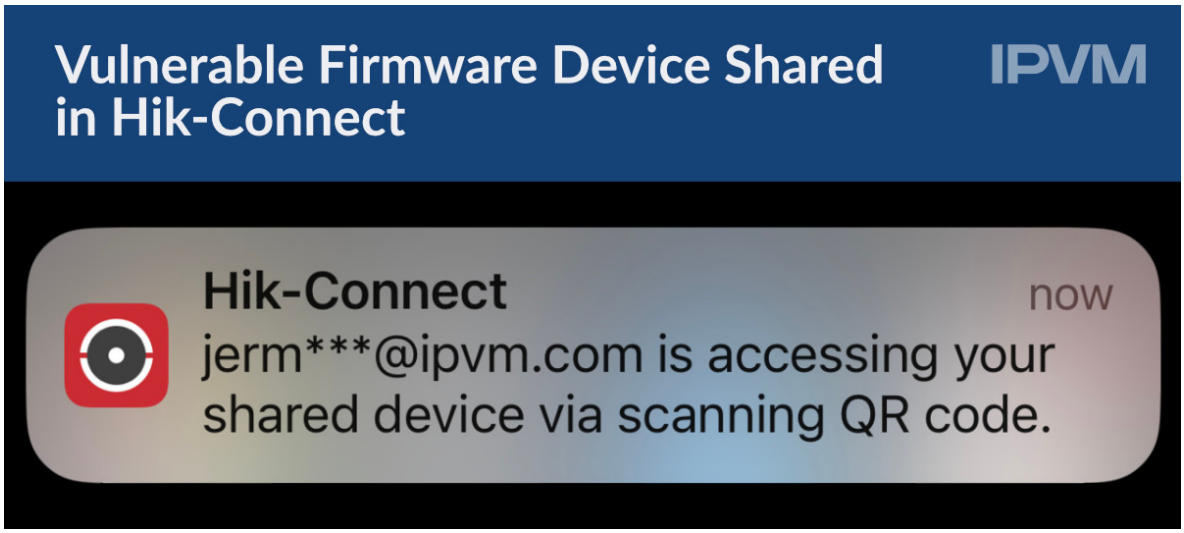
However, shared QR codes for direct connection to the Hikivsion IP camera using the Hik-Connect app do not require encryption passwords for video feeds.

The encryption password only helps those with Hik-Connect enabled. Cameras do not need this to be enabled to be added to Hik-Connect if port forwarding is configured.

Hik-Connect Works on Old Vulnerable Firmware

Compounding the Hik-Connect abuse issue is the fact that old, vulnerable firmware is able to use Hik-Connect without any restrictions beyond current firmware devices.

IPVM tested sharing a camera running firmware vulnerable to the [Hikvision backdoor magic string](#).



For more, see [Hikvision's Hik-Connect Cloud Connects To Vulnerable Devices](#)

IPVM Recommended Changes Hikvision Should Implement

While the changes above do make sharing more difficult / limited, they don't make a critical impact. There are several changes that Hikvision can make that would have more impact in disrupting unauthorized sharing.

- *Require Remote Access Setup in Person:* Making it so that the user needs to physically be with the device being shared to set up sharing would prevent others from scanning the web and collecting cameras from around the world to be shared.
- *AAA (Authentication, Authorization, and Accounting):* Verify users with sharing access are legitimate device owners, not bad actors. Adding an email or phone number to login to the device would help. Adding 2FA would help protect that. Ensuring that people only have access to what they should. Logging the access of authenticated and authorized users, collecting Hik-Connect account details and IP addresses of those remotely viewing via Hik-Connect.
- *Notifications:* Ensuring that legitimate device owners are notified. This can be done via OSD or other methods. The current push notifications will not be effective since Hik-Connect does not even need to be enabled on the device for a bad actor to add the camera to their app. They can simply use

the IP to add.

No Response from Hikvision

IPVM emailed Hikvision's media team and two other Hikvision employees, but Hikvision did not respond. If Hikvision responds, we will update the report and add a comment.

Software Version Tested

Hik-Connect Version: 5.2.3.20230823

Comments (1)

John Honovich IPVM |

While Hikvision deceptively markets its cybersecurity based on grossly misleading and easily manipulated CVE counts, this is an excellent example of very bad design decisions by Hikvision that enable hacking and criminal activity to be facilitated by Hikvision's cloud.

Generated for Charles Rollet on Aug 02, 2024 for Your Use Only - No Sharing - No Promotions