Detected extremely serious vulnerability in Hikvision security cameras

Successfully exploiting this vulnerability helps hackers gain access to the camera and the victim's network.

Recently, British security research firm Watchful IP has reported a serious security flaw in Hikvision's cameras. This vulnerability, assigned code CVE-2021-36260, is rated 9.8 points, becoming the most serious camera vulnerability ever.

According to Watchful IP, a hacker exploiting this vulnerability can control the camera and the victim's internal network. Hackers will have access to more than what users have on their devices. In addition, hackers can also execute remote code (RCE) without any interaction of the victim.

This is a very serious problem, Watchful IP says. The reason is because Hikvision is the largest security camera brand in the world. Their products are used globally by both ordinary consumers, businesses and government agencies and organizations.

Watchful IP also adds that this vulnerability may exist in Hikvision's firmware since 2016.

Hikvision quickly released a security advisory regarding this issue. In it, the company acknowledged what Watchful IP reported and revealed a list of camera models that may be affected. This list includes more than 80 camera models, so the number of affected users and customers will be very large.

Hikvision recommends that users and their customers update to the latest firmware as soon as possible to prevent security risks. Currently, the new firmware version has been posted on the company's homepage.

So far Hikvision has not had a way to automatically update the new firmware version.