
CYFIRMA
DECODING THREATS
Thousands of
Hikvision Cameras
are still vulnerable and
can be potentially exploited

Introduction

CYFIRMA researchers have observed, as per the sample analysed, thousands of Hikvision cameras still being used, which are vulnerable and could be exploited by cybercriminals.

Hangzhou Hikvision Digital Technology Co., Ltd., often shortened to Hikvision, is a Chinese state-owned manufacturer and supplier of video surveillance equipment for civilian and military purposes, headquartered in Hangzhou, Zhejiang. Hikvision is a provider of Industrial IoT sensors technologies, and active in the education, and retail industries, amongst other critical infrastructure segments.

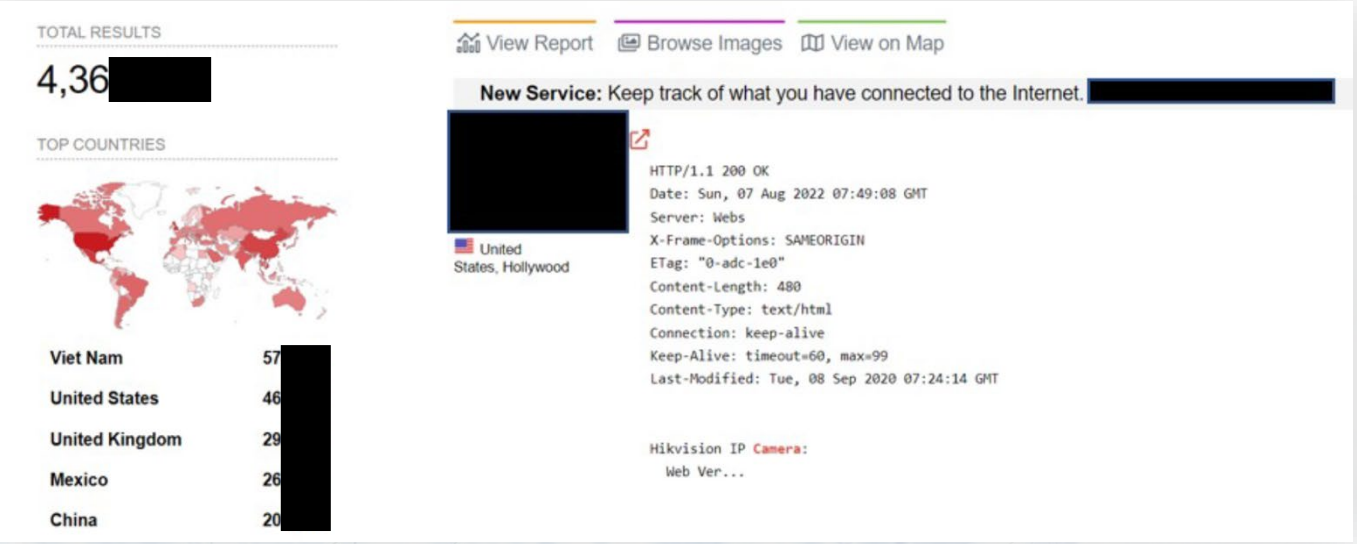


Fig: Global Deployment Landscape (July 2022)

As per researchers, by 2025, 30% **Critical Infrastructure organizations** could experience a security breach.

Source: Gartner

Thousands of Hikvision Cameras are still vulnerable and can be potentially exploited

Observations in the Underground Forums

CYFIRMA researchers have observed in the sample analysed, multiple instances of hackers looking to collaborate on exploiting Hikvision cameras using the command injection vulnerability (CVE-2021-36260) globally.

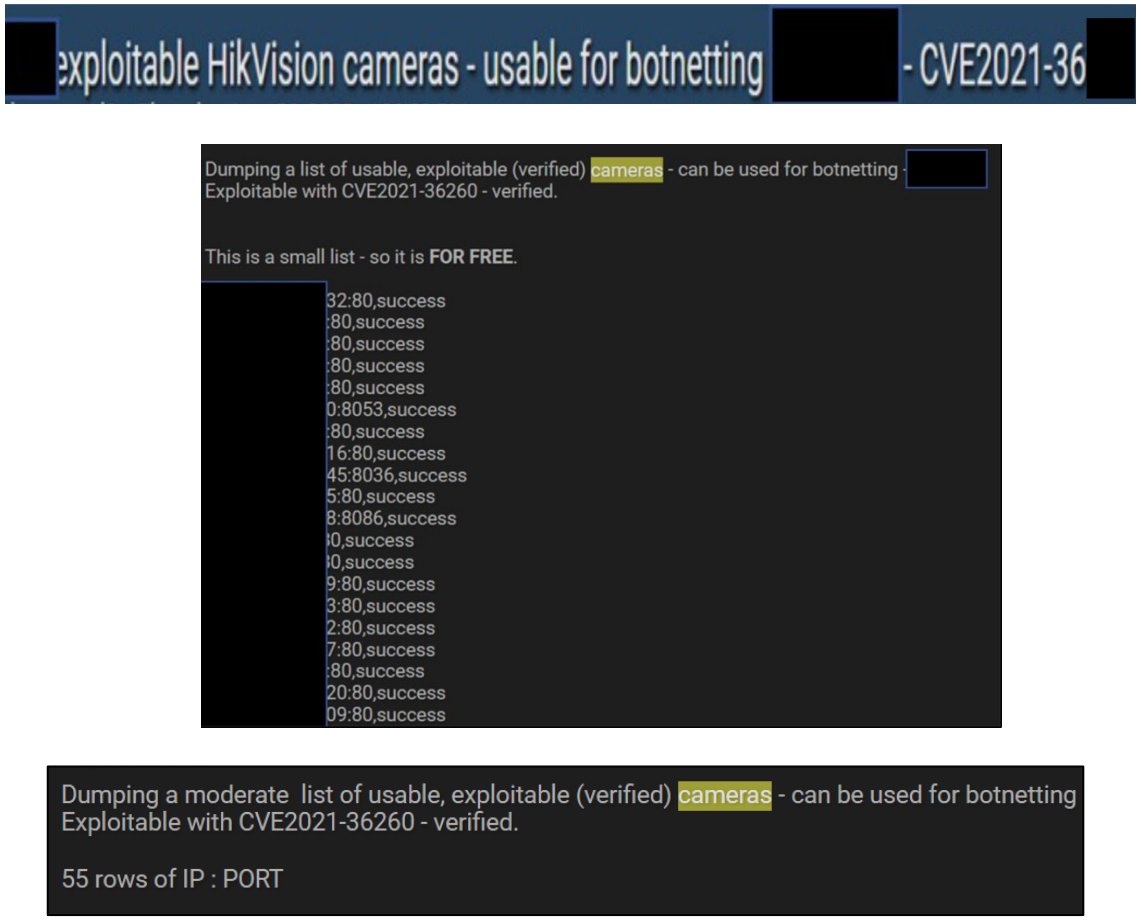


Fig: Screenshots from underground forums

Specifically in the Russian forums, we have observed **leaked credentials** of Hikvision camera products available for sale. These can be leveraged by hackers to gain access to the devices and exploit further the path of attack to target an organization's environment.

Credential Leaks observed in Dark Web Forums

Thousands of Hikvision Cameras are still vulnerable and can be potentially exploited

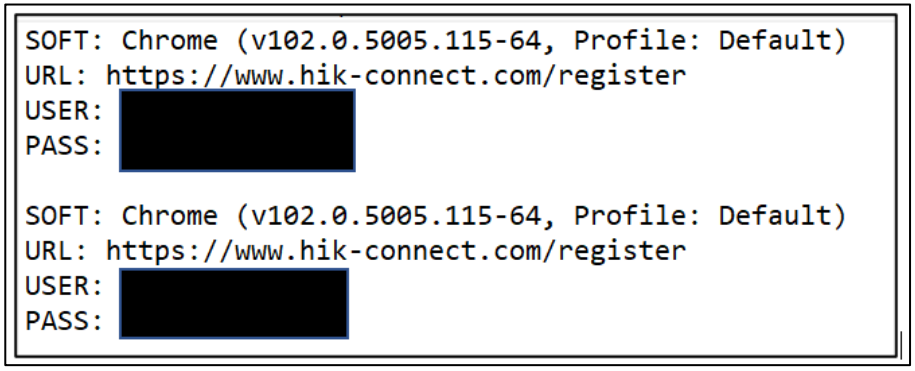


Fig: Screenshot from Russian forums with sample data

About the command injection vulnerability CVE-2021-36260

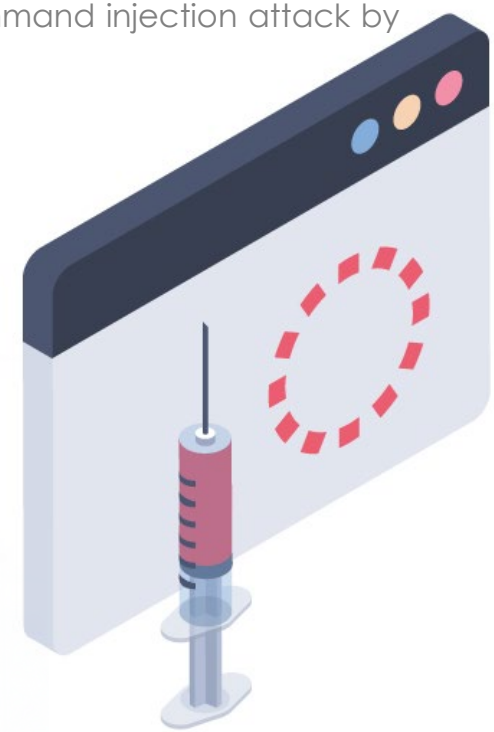
About a year ago, a critical command injection vulnerability impacted the web server of some Hikvision products – was identified as CVE-2021-36260. An attacker could exploit the vulnerability and carry out a command injection attack by sending some messages with malicious commands due to insufficient input validation.

Details of the vulnerability are as follows:
CVE No: CVE-2021-36260
CVSS Score: 9.8
Exploits: Link (Feb 2022), Link (Oct 2021)

MITRE ATT&CK Framework:

Sr.No	Tactics	Techniques
1	TA005: Defense Evasion	T1202: Indirect Command Execution

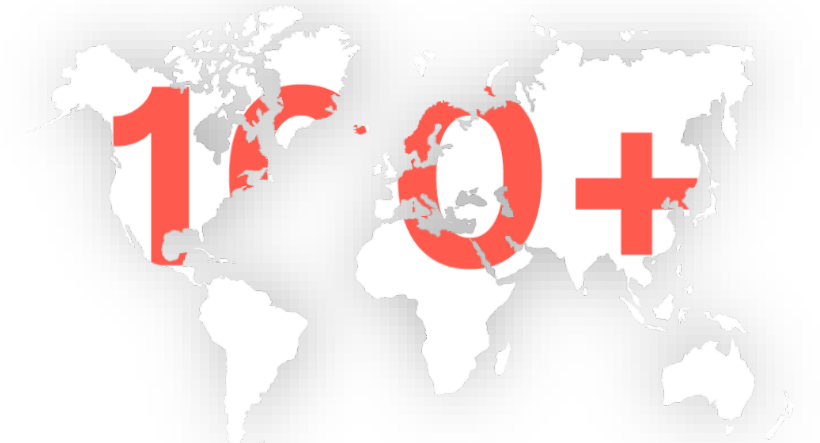
Source: NVD, Vul Db



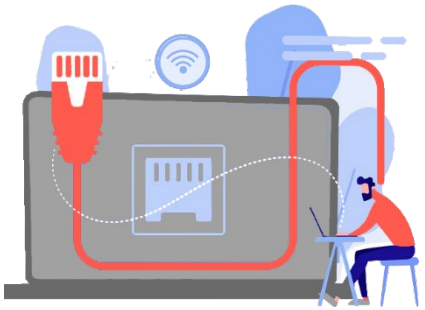
Research & Analysis

CYFIRMA researchers have observed in the sample analysed, multiple open ports which seem to be in use for Hikvision cameras. These open ports could act as the initial access broker for cybercriminals.

Following summarizes our analysis of a sample of ~285K as of July 2022.

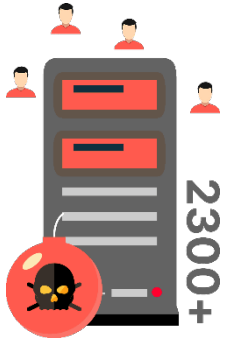


100+ Nations Impacted



450+ Non-standard Ports

Devices still Vulnerable



Organizations Impacted

Thousands of Hikvision Cameras are still vulnerable and can be potentially exploited

GEOGRAPHICAL SPREAD OF NUMBER OF DEVICES

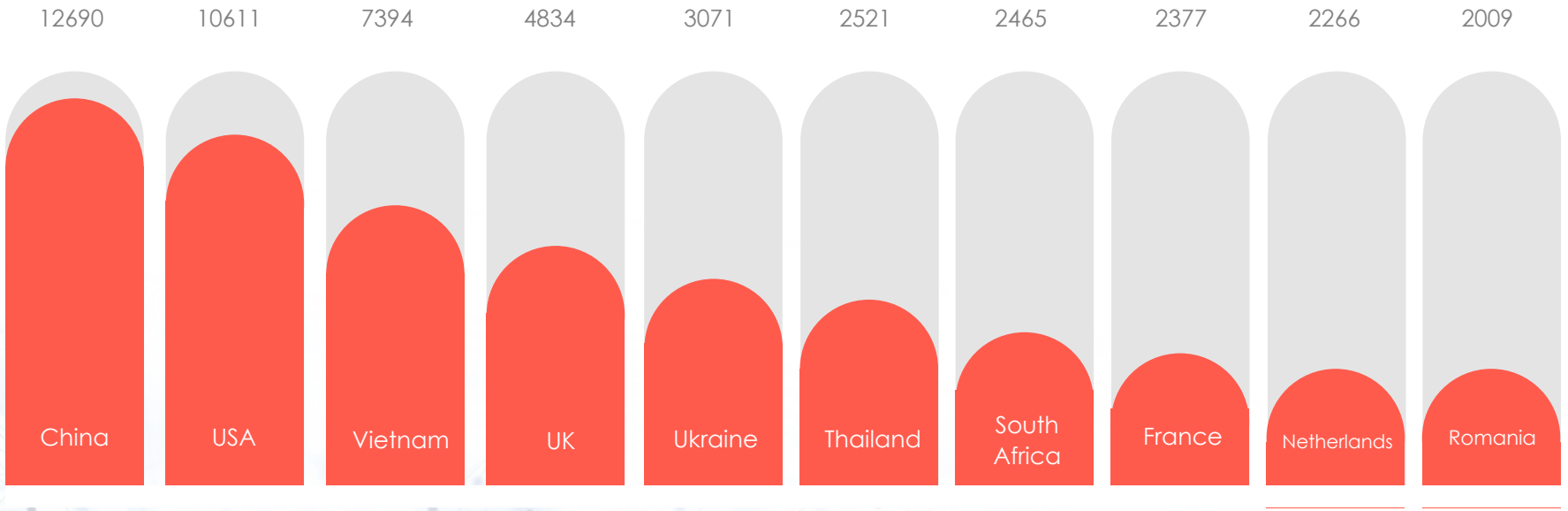


Fig: Top 10 nations using Hikvision camera products (as per the sample analysed)

Thousands of Hikvision Cameras are still vulnerable and can be potentially exploited

Attribution & Correlation

Every hacker group could potentially exploit vulnerabilities in these devices, although any specific cybercriminal group exploiting these cannot be isolated at this stage. However, we have reasons to believe that - Chinese threat groups such as MISSION2025/APT41, APT10 and its affiliates, as well as unknown Russian threat actor groups could potentially exploit vulnerabilities in these devices to fulfil their motives (which may include specific geo-political considerations).

In drawing a parallel with indicators CYFIRMA research team has been observing since August 2021, a threat actor group was observed launching a cyberespionage campaign called "think pocket" exploiting a popular connectivity product. The campaign was found to be targeting industries including – Telecommunication & Infrastructure, Energy Production & Supply, Defense, Government, Research, Automobile, Manufacturing, ICT, and Trading. Geographies being targeted included - United States, Japan, Philippines, Taiwan, United Kingdom, Thailand, Australia, India, and many more.

In another instance, unknown Russian threat actor groups were observed launching a cyber-attack campaign exploiting 1512 a specific and popular brand of routers. Industries targeted by the campaign included - Chemical & Large Manufacturing, Fertilizer & Tire, Electronic Product Equipment, Healthcare, Shipping & Transportation, and Polymer & Fibre. Geographies being targeted included - France, Germany, Ukraine, Japan, Indonesia, UK, India, USA, Latvia, Taiwan, and many others.

From an External Threat Landscape Management (ETLM) analogy, cybercriminals from countries that may not have a cordial relation with other nations, could use the vulnerable Hikvision camera products to launch a geo-politically motivated cyber warfare. Cyber criminals and state-sponsored hacker groups could very easily collaborate using this avenue as an opportunity for mutual gains and to further their interests.

Thousands of Hikvision Cameras are still vulnerable and can be potentially exploited

Conclusion

Given the current geopolitical driven cyberwarfare brewing across the world, we suspect an uptick in cyberattacks from various nation-state threat actors on critical infrastructure, state entities, defence organizations, and many more. Open vulnerabilities and ports in such devices will only compound the impact on targeted organizations and their countries economic and state prowess.

It is paramount to patch the vulnerable software of the Hikvision camera products to the latest version. Organizations need to adopt a ETLM powered risk-based approach to cybersecurity decision making to minimize possible exposures and threats coming their way.

By 2023 financial impact on OT and other cyber-physical systems will be over USD 50 Billion

Source: Gartner

Thousands of Hikvision Cameras are still vulnerable and can be potentially exploited

CYFIRMA is an External Threat Landscape Management (ETLM) platform company. We combine cyber intelligence with attack surface discovery and digital risk protection to deliver early warning, personalized, contextual, outside-in, and multi-layered insights. Our cloud-based AI and ML-powered analytics platform provides the hacker's view with deep insights into the external cyber landscape, helping clients prepare for impending attacks. CYFIRMA is headquartered in Singapore with offices across APAC, US and EMEA. The company is funded by Goldman Sachs, Zodius Capital, and Z3 Partners.

www.cyfirma.com