IPVM

August 17, 2021

Cybersecurity of Surveillance IoT Devices Under Executive Order 14028, Improving the Nation's Cybersecurity

IPVM Contact: Conor Healy, chealy@ipvm.com

Virtually all US facilities are covered by surveillance networks with historically high vulnerabilities, making them one of IoT's highest-risk categories. Hundreds of US sellers hide the origins of their software and hardware, creating exactly the kind of pressing cybersecurity risks that the Executive Order seeks to address. NIST and the FTC are positioned to solve this problem by requiring labelling of surveillance and other IoT devices with clear disclosures of the original software provider. We suggest this be a top priority in carrying out the EO, and outline the problem in more detail below.

Surveillance vulnerability risks extend far beyond interrupting the function of surveillance systems. They collect and store sensitive data on countless millions of Americans each year, including everything from police interviews to biometric profiles. Additionally, surveillance is often part of internal networks running important infrastructure, such as public utilities, meaning vulnerabilities can be exploited to catastrophic effect. (The high-profile breach of Verkada in March positioned hackers to pivot to other systems in exactly this way.[1])

Despite these risks, surveillance supply chains lack transparency. Companies regularly refuse to disclose the origin of their products. IPVM's own testing engineers routinely discover products are relabelled but it often requires buying products and tearing them down, an impractical process for the average user.

This problem occurs because the manufacturers and end-users are often separated by intermediaries relabelling products under their own brands. In passing these products off as their own, they are incentivized to resist questions about their true origins.

The result is that cybersecurity professionals are often unable to answer a basic question: who made our surveillance devices and software? This impedes a proper risk assessment, which should consider whether hardware/software comes from a reputable source, and if any vulnerabilities are known to exist for their products. Furthermore, it means end-users do not know where to go with questions about their devices, and this could impede a swift reaction when a cyberattack occurs.

A real world example is Honeywell's Performance Series line of surveillance cameras, whose hardware and software are made by Dahua. On the next page is a side-by-side comparison of one of these cameras and its software, which are identical other than logos and the camera's casing. In recent years, researchers have discovered multiple cybersecurity vulnerabilities in Dahua devices. Moreover, Congress banned Dahua for Federal purchases over cybersecurity risks in the 2019 NDAA, and the FCC recently passed an NPRM to strip Dahua's authorizations over these same risks. These are clearly material facts for any cybersecurity risk assessment. Still, Honeywell sells the Performance Series under their own brand with no mention of Dahua in product materials.

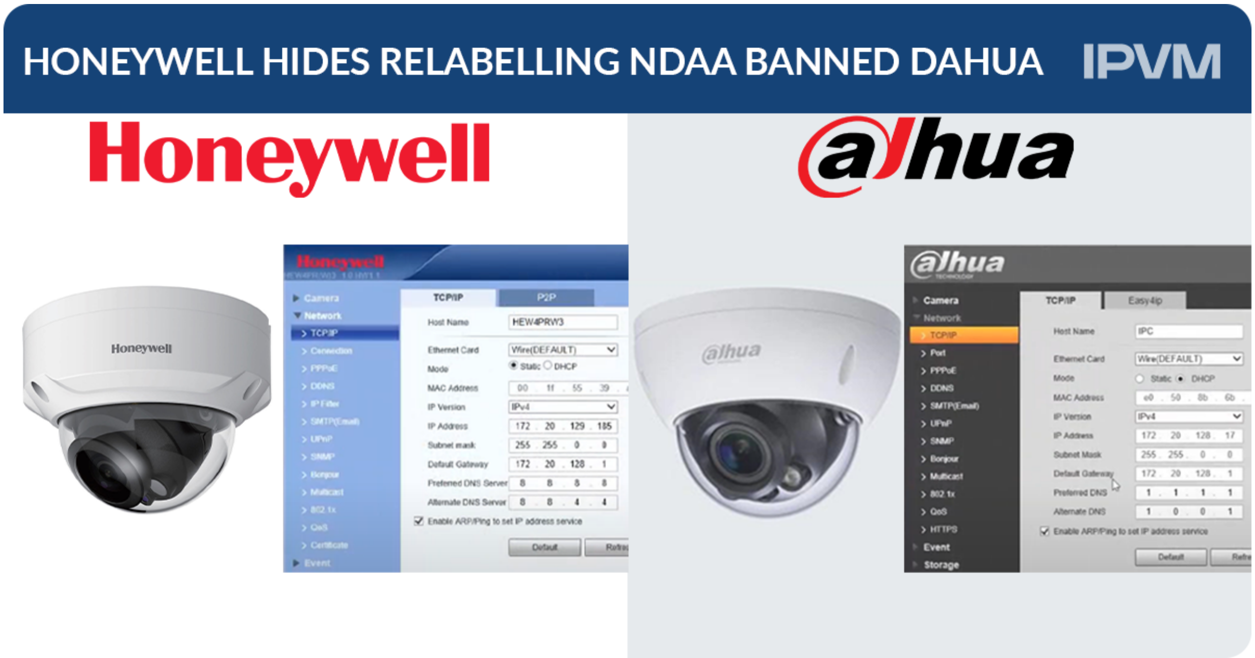
Just limited to surveillance manufacturers banned under the 2019 NDAA, there are greater than 100 brands selling relabelled surveillance products, and perhaps thousands of available models[2][3]. Many were even unwittingly listed on GSA Advantage as recently reported by IPVM and The Intercept, violating the Federal law.[4]

NIST and the FTC can solve this problem by requiring clear disclosure of the original manufacturer and developer of IoT hardware/software as part of cybersecurity labelling. This is information that all sellers of surveillance already know, or ought to know. Such a requirement is practical, and not burdensome, to manufacturers and distributors. Extending this requirement to cover critical components prone to exploitation, such as SOCs, should also be considered.

An overview of IPVM is provided below. We welcome any questions or further opportunities for our experts to provide information about surveillance technology, or the surveillance industry. Correspondence may be addressed to Conor Healy, chealy@ipvm.com.

About IPVM

IPVM is a research organization focused on businesses and technologies in surveillance, security, face recognition, biometrics, thermography, and more. We are funded by 15,000 paying members under a Consumer Reports-like model. IPVM operates a 12,000 sq ft testing facility in Bethlehem, PA staffed with experts evaluating new products and publishing performance reports for our subscribers. In addition to testing, IPVM analysts publish 3-4 articles each weekday featuring everything from business news to investigative reporting. Our work is cited by Congress, and regularly covered in the national press.



Host Name HEW4PRW3
Ethernet Card Wire(DEFAULT)
Mode ● Static ○ DHCP
MAC Address 00 . 11 . 55 . 39 .
IP Version IPv4
IP Address 172 . 20 . 129 . 185
Subnet mask 255 . 255 . 0 . 0
Default Gateway 172 . 20 . 128 . 1
Preferred DNS Server 8 . 8 . 8 . 8
Alternate DNS Server 8 . 8 . 4 . 4
☑ Enable ARP/Ping to set IP address service

Host Name IPC
Ethernet Card Wire(DEFAULT)
Mode ○ Static ● DHCP
MAC Address e0 . 50 . 8b . 6b .
IP Version IPv4
IP Address 172 . 20 . 128 . 17
Subnet Mask 255 . 255 . 0 . 0
Default Gateway 172 . 20 . 128 . 1
Preferred DNS 1 . 1 . 1 . 1
Alternate DNS 1 . 0 . 0 . 1
☑ Enable ARP/Ping to set IP address service

[1] Turton, W. “Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals”, *Bloomberg*, 9 March 2021, <https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams>

[2] “Hikvision OEM Directory,” *IPVM, 3* June 2021. <https://ipvm.com/reports/hik-oems-dir>

[3] “Dahua OEM Directory,” *IPVM,* 5 May 2021. <https://ipvm.com/reports/dahua-oem>

[4] Biddle, S. “U.S. Military Bought Cameras In Violation of America’s Own China Sanctions,” *The Intercept,* 20 July 2021. <https://theintercept.com/2021/07/20/video-surveillance-cameras-us-military-china-sanctions>