Contact: 647-872-9982
Toll-free/Fax: 1-844-247-6633

Email: info@relaymedical.com
65 International Blvd. Suite 202
Etobicoke, Ontario M9W 6L9

Relay Addresses the Recent Cybersecurity Vulnerability in Surveillance and Security Cameras market; 100 Million Connected Devices Susceptible to Remote Hijacking

TORONTO, September 24, 2021 – Relay Medical Corp. ("**Relay**" or the "**Company**") (**CSE: RELA, OTCQB: RYMDF, Frankfurt: EIY2**) addresses a recent revelation about the widely-used Hikvision[1], a Chinese state-owned surveillance and connected security camera manufacturer, whereby a critical vulnerability was discovered in more than 100 million connected devices currently operational in the market.

The Hikvision vulnerability affects dozens of IoT device companies, including devices affiliated with brands such as Toshiba, Honeywell, Panasonic, Hyundai and Hitachi.[2] Hikvision owns approximately 40% of the global surveillance and security camera market.[3] Hikvision has admitted a 9.8 vulnerability score which is "the highest level of critical vulnerability" and is estimated to impact more than 100 million connected devices operating in the market.[4]

"Recent Hikvision news demonstrates a widespread problem of software weaknesses and vulnerabilities that are hidden in the software components of connected products this is meant to be addressed by NTIA (National Telecommunications and Information Administration) and its SBoM software transparency initiative. It's another example of why software and hardware companies need to have internal product security hygiene and processes in place that provide a singular, transparent view into all their products. Cybeats offers holistic supply chain security starting from the design phase, while also continuously assessing, monitoring and eliminating threats in real-time of critical operating devices" ***said Dmitry Raidman, CTO and Co-founder of Cybeats.***

Cybeats Provides Preventative Solutions

Cybeats products directly address the Hikvision vulnerability by providing secure by design and SBoM management capabilities, and we recommend:

[1] https://us.hikvision.com/en
[2] https://ipvm.com/reports/hik-oems-dir
[3] https://www.forbes.com/sites/leemathews/2021/09/22/widely-used-hikvision-security-cameras-vulnerable-to-remote-hijacking/?sh=6e12f1502f31
[4] https://ipvm.com/reports/hik-oems-dir

Contact: 647-872-9982
Toll-free/Fax: 1-844-247-6633

Email: info@relaymedical.com
65 International Blvd. Suite 202
Etobicoke, Ontario M9W 6L9

A) Product vendors and manufacturers to start integrating SBoM generation in their processes earlier in manufacturing and development stages

B) Product consumers should start requesting the SBoMs for products they procure and resell, including any white labeled devices such as currently vulnerable Hikvision security products

C) Both manufacturers and consumers will need to start utilizing SBoM for various security and compliance use-cases, as regulatory mandates on software & SBoM are a widespread requirement

Malwarebytes[5] identified that Original Equipment Manufacturers (OEMs) rebrand Hikvision cameras and sell them as their own. It could take quite some time before all of these other potentially vulnerable devices are identified. Hikvision is PRC government-owned[6] but banned by the US-government[7]. It is the world's largest video surveillance manufacturer and a generally hidden supply chain to many Western companies. Given the deployment of these cameras at sensitive sites, critical infrastructure is potentially at risk.

Cybeats Provides Active Defense Solutions

Having the Cybeats agent integrated into a connected device, such as those affected by this Hikvision vulnerability, would have provided real-time actionable protection to affected brands that were identified by ipvm[8], such as Toshiba, Honeywell, Panasonic, Hyundai and Hitachi. Cybeats supports manufacturers (such as surveillance and security camera companies) to build connected devices with security in mind, beginning in the design phase throughout the product life-cycle. Lastly, Cybeats IoT RASP capabilities can provide actionable data about the device's operating state, and allow for threat elimination in real-time as new attacks emerge. Once a device vulnerability is found, Cybeats's SBOM Studio can provide insight into which devices are affected, and which to recall or which to provide a firmware update. This provides manufacturers with fleet management tools along with efficient and accurate firmware updates to the affected devices.

[5] https://blog.malwarebytes.com/exploits-and-vulnerabilities/2021/09/patch-now-insecure-hikvision-security-cameras-can-be-taken-over-remotely/
[6] https://ipvm.com/reports/hikvision-prc
[7] https://ipvm.com/reports/aug-13-2019
[8] https://ipvm.com/reports/hik-oems-dir

Contact: 647-872-9982
Toll-free/Fax: 1-844-247-6633

Email: info@relaymedical.com
65 International Blvd. Suite 202
Etobicoke, Ontario M9W 6L9

Other Recent Cyber Attacks

IoT cyber attacks have escalated in 2021[9], according to Kaspersky[10]. IoT cyberattacks more than doubled with roughly 1.5 Billion IoT attacks occurring from January to June 2021. The study was conducted using software honeypots[11], which emulate IoT devices as a proxy for vulnerable hardware endpoints. The findings also confirm that the pandemic has exacerbated IoT vulnerabilities by prolonging device usage in household settings. Many of these devices – whether intended for enterprise or personal use – lack adequate security protocols.[12]

This Hikvision vulnerability news also follows the breach of Tesla[13] security cameras, which came along with the hacking of jails and hospitals. The live feeds and data of 150,000 surveillance cameras, collected by Silicon Valley startup Verkada Inc., were breached in March 2021.[14] Vulnerabilities like these can result in significant service disruptions, as exemplified in the Mirai botnet attack[15] from 2016 whereby the hackers used a botnet of IoT devices including webcams, routers, and DVRs to 'take down' the internet in North America for multiple days. Many prominent corporations, including CNBC, Amazon, Twitter, Netflix, Spotify, and Paypal, experienced outages of their website and client server issues, causing shutdowns and service delays lasting several hours.[16]

RECENT NEWS: Relay shares the highlights from their Cybeat's SBoM webinar, where notable NTIA past and present employees, Allan Friedman and Tom Alrich, respectively, participate in the discussion about the State of Cybersecurity. The highlights and YouTube recording can be found here: https://bit.ly/3hZTh82.

SUBSCRIBE: For more information on Relay or to subscribe to the Company's mail list visit: https://www.relaymedical.com/news

About Relay Medical Corp.

[9] https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky
[10] https://www.kaspersky.ca/
[11] https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot
[12] https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky
[13] https://www.tesla.com/
[14] https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams
[15] https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/
[16] https://www.cnbc.com/2016/10/21/major-websites-across-east-coast-knocked-out-in-apparent-ddos-attack.html

Contact: 647-872-9982
Toll-free/Fax: 1-844-247-6633

Email: info@relaymedical.com
65 International Blvd. Suite 202
Etobicoke, Ontario M9W 6L9

Relay Medical is a technology innovator headquartered in Toronto, Canada focused on the development of novel solutions in the diagnostics, AI data science and IoT security sectors. Relay recently acquired Cybeats Technologies, a platform which offers a holistic approach to cybersecurity and addresses the $73 billion IoT security market through their Software Bill of Materials and microagent solution. Cybeats provides real-time cybersecurity for connected devices, critical infrastructure, automotive, medical and IoT (Internet of Things) sectors.

The Company held a Special Meeting to approve a Name Change on September 20, 2021 as the Company's core competencies and product offerings have organically grown beyond the medical device industry, and this expansion into new industries and businesses will be reflected in the Name Change. The Company's new name will more aptly and effectively communicate the business and its commercial verticals.

Website: www.relaymedical.com

Contact:

Destine Lee
Media & Communications
Relay Medical Corp.
Office. 647-872-9982
TF. 1-844-247-6633
Media Inquiries: media@relaymedical.com
Investor Relations: investor.relations@relaymedical.com

Bernhard Langer
EU Investor Relations
Office. +49 (0) 177 774 2314
Email: blanger@relaymedical.com

Forward-looking Information Cautionary Statement

Except for statements of historic fact, this news release contains certain "forward-looking information" within the meaning of applicable securities law. Forward-looking information is frequently characterized by words such as "plan", "expect", "project", "intend", "believe", "anticipate", "estimate" and other similar words, or statements that certain events or conditions "may" or "will" occur. Forward-looking statements are based on the opinions and estimates at the date the statements are made, and are subject to a variety of risks and uncertainties and other factors that could cause actual events or results to differ materially from those anticipated in the forward-looking statements including, but not limited to delays or uncertainties with regulatory approvals, including that of the CSE. There are uncertainties inherent in

Contact: 647-872-9982
Toll-free/Fax: 1-844-247-6633

Email: info@relaymedical.com
65 International Blvd. Suite 202
Etobicoke, Ontario M9W 6L9

forward-looking information, including factors beyond the Company's control. There are no assurances that the commercialization plans for the technology described in this news release will come into effect on the terms or time frame described herein. The Company undertakes no obligation to update forward-looking information if circumstances or management's estimates or opinions should change except as required by law. The reader is cautioned not to place undue reliance on forward-looking statements. Additional information identifying risks and uncertainties that could affect financial results is contained in the Company's filings with Canadian securities regulators, which filings are available at www.sedar.com.