Global Headquarters

Genetec Inc.
2280 Alfred Nobel Blvd.
Montreal, Quebec H4S 2A4
Canada

T: +1 514.332.4000

Media Alert

New Genetec research shows almost 4 in 10 security cameras can be at risk of cyber-attack due to outdated firmware

Genetec primary data also shows that almost 1 in 4 organizations rely on default passwords for their security cameras

MONTRÉAL, December 5 2019— Outdated camera firmware, and failing to change default passwords present some of the biggest weaknesses in cybersecurity defense. As the number of interconnected security devices keeps on growing, keeping pace with the latest updates can be tricky and very time-consuming. According to new research* conducted by Genetec Inc. ("Genetec"), a leading technology provider of unified security, public safety, operations, and business intelligence, as many as 68.4%—or almost 7 out of 10—cameras are currently running out of date firmware.

Installing the latest firmware is not just about accessing exciting new features, warns Genetec. It ensures the latest cybersecurity protection measures are implemented as soon as they become available, a crucial step in ensuring an organization's resilience against cyber-attacks.

"Our primary research data points to the fact that more than half of the cameras with out of date firmware (53.9%) contain known cyber security vulnerabilities. By extrapolating this to an average security network, nearly 4 out of every 10 cameras are vulnerable to a cyber-attack," said Mathieu Chevalier, Lead Security Architect at Genetec.

The research conducted by Genetec also showed that nearly 1 in 4 organizations (23%) fail to use unique passwords, relying instead on the same password across all cameras from the same manufacturer, leaving an easy point of entry for hackers once only one camera has been compromised.

Until recently, IP cameras came with default security settings, including admin login information that is often publicly available on the manufacturers' websites. While most camera

manufacturers now request users to set up a new password and admin credentials at installation, businesses, cities and government organizations with older equipment never updated their passwords, potentially compromising the other critical data and systems that reside on their network.

“Unfortunately, our research shows that the “set it and forget it” mentality remains prevalent putting an entire organization’s security and people’s privacy at risk. All it takes is one camera with obsolete firmware or a default password to create a foothold for an attacker to compromise the whole network,” added Chevalier. “It is critical that organizations should be as proactive in the update of their physical security systems as they are in updating their IT networks.”

For more information about how to keep your infrastructure cyber secure, please visit: https://resources.genetec.com/cybersecurity

*Source: Research conducted on a sample of 44,763 cameras connected to systems that are part of the Genetec opt-in product improvement program.

About Genetec

Genetec Inc. is an innovative technology company with a broad solutions portfolio that encompasses security, intelligence, and operations. The company’s flagship product, Security Center, is an open-architecture platform that unifies IP-based video surveillance, access control, automatic license plate recognition (ANPR), communications, and analytics. Genetec also develops cloud-based solutions and services designed to improve security, and contribute new levels of operational intelligence for governments, enterprises, transport, and the communities in which we live. Founded in 1997, and headquartered in Montreal, Canada, Genetec serves its global customers via an extensive network of resellers, integrators, certified channel partners, and consultants in over 80 countries.

For more information about Genetec, visit: www.genetec.com

Press Contacts:

North America
Véronique Froment
HighRez
Veronique@highrezpr.com
Tel: +1 603.537.9248