UNLOCKED THREATS:

Counterintelligence Vulnerabilities in Commercial Electronic Locks and Considerations to Protect Sensitive Information

Commercial electronic lock systems are a first line defense used by companies to protect some of their most vital assets, including trade secrets, intellectual property, business intelligence, and personally identifiable information. However, commercial electronic locks may face serious national security risks from foreign intelligence services, non-traditional collectors, and others who use various methods to illicitly acquire U.S. sensitive information at the expense of U.S. industry. To mitigate these risks, the American public and our allies are encouraged to choose commercial safe locks that provide robust protection for sensitive information. The information in this bulletin is meant to help reduce the likelihood of compromise while reminding companies to remain vigilant against non-traditional collectors and foreign intelligence services threats.

POTENTIAL VULNERABILITIES

Commercial electronic locks often incorporate wireless communication protocols like Bluetooth Low Energy (BLE) and Wi-Fi, which are susceptible to well-documented vulnerabilities including signal interception, spoofing, and replay attacks. These weaknesses can enable unauthorized remote access, manipulation of lock states, or extraction of credentials through packet sniffing or brute-force techniques, especially if encryption and authentication mechanisms are poorly implemented. Additionally, these locks may contain physical and software vulnerabilities, including but not limited to:

- Inadequate or compromised firmware that lacks proper security patches or uses outdated cryptographic standards
- Mechanical design flaws that can lead to premature hardware failures
- Embedded manufacturer reset codes intended for diagnostics or customer support, which may be exploited if not properly secured and stored.

Electronic locks may face further risks tied to their country of origin and the global sourcing of components. For example:

- Chinese-made locks may harbor undisclosed reset codes and firmware backdoors – vulnerabilities that could be exploited under China's surveillance laws.
- Assembly in regions with inconsistent regulations, standards, and cybersecurity capabilities – such as Southeast Asia, as well as emerging hubs like India and Brazil – can lead to tampering (i.e. cloned chips or compromised authentication) and may exacerbate other vulnerabilities.
- Parts for electronic locks manufactured in countries with weak oversight or adversarial interests can introduce vulnerabilities during production or distribution.

Spanning all of this, Russia, Iran, and North Korea's cyber espionage efforts are known to focus on vulnerabilities that allow them access to U.S. industry and critical infrastructure. These risks threaten intellectual property, client data, and operational integrity.

MITIGATION

Commercial locks are the first line of defense for your business—but not all locks are created equal. To safeguard your assets, it is essential to take a proactive approach to lock security. Start by investing in high-security commercial locks that resist picking, drilling, and unauthorized key duplication.

- Look for locks that meet recognized standards such as ANSI/BHMA Grade 1, FIPS 140-2, or other industry certifications for locks that meet rigorous resistance standards against forced entry and manipulation.
- Be especially cautious with locks that rely on remote-access technologies such as cloud-based control panels, mobile apps, or wireless connectivity. While these features offer convenience, they also introduce new attack surfaces that can be exploited through network vulnerabilities, compromised credentials, or supply chain tampering.
- Whenever possible, opt for offline electronic locks or air-gapped systems that eliminate remote access vectors. If remote functionality is essential, ensure it is protected by end-to-end encryption, multi-factor authentication, and regular firmware updates from trusted vendors.
- Conduct regular security audits to identify outdated or vulnerable locks, and replace them with modern alternatives like restricted key systems or hardened electronic locks.
- Work with certified locksmiths who can assess entry points, recommend upgrades, and implement master key systems to limit access.
- Complement your locks with layered security measures such as surveillance cameras, alarm systems, and strict visitor protocols.

And most importantly, demand full supply chain transparency from vendors – know where your lock components are made, and avoid products from manufacturers subject to foreign government control or lacking cybersecurity certifications. By combining strong hardware with smart policies, and minimizing reliance on remote-access technologies, you can dramatically reduce the risk of lock-based breaches and keep your business secure.

REPORTING INCIDENTS

- If you are concerned with an immediate threat to you or your facility, contact local law enforcement.
- If you believe your company or its operations have been targeted by or are at risk from foreign threat actors, contact the Private Sector Coordinator at your local FBI Field Office: www.fbi.gov/contact-us/field-offices. You can also visit https://tips.fbi.gov or call **1-800-CALL-FBI**.
- For additional information on NCSC threat awareness materials or publications, visit www.ncsc.gov or contact NCSC_Outreach@odni.gov.