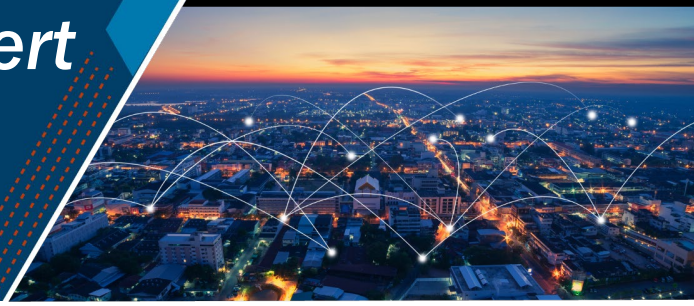
Secure by Design Alert

How Manufacturers Can Protect Customers by Eliminating Default Passwords



Malicious Cyber Actors Exploit Default Passwords

Malicious cyber actors continue to exploit default passwords (e.g., "1234," "default," "password") on internet-exposed systems to gain initial access to, and move laterally within, organizations. Threat actors, including Islamic Revolutionary Guard Corps (IRGC)-affiliated actors,[1] have been successful in compromising critical infrastructure systems in the United States by exploiting operational technology (OT) products sold by manufacturers with passwords set to a static default. CISA is releasing this Alert—based upon recent and ongoing threat activity—to urge every technology manufacturer to eliminate default passwords in the design, release, and update of all products. Years of evidence have demonstrated that relying upon thousands of customers to change their passwords is insufficient, and only concerted action by technology manufacturers will appropriately address severe risks facing critical infrastructure organizations.

While threat actors affiliated with the Iranian Government's Islamic Revolutionary Guard Corp have made headlines recently by exploiting default passwords, the guidance for vendors to use alternatives to default passwords is not new. CISA and others in the cybersecurity community have been issuing similar warnings for years, but the harm imposed on customers continues. Now is the time for every technology manufacturer to take action.

Secure by Design Lessons to Learn

A core tenet of secure by design is that manufacturers create safe and secure default behavior in products provided to customers. The use of widely known default passwords is unacceptable given the current threat environment. Studies by CISA show that the use of default credentials, such as passwords, is a top weakness that threat actors exploit to gain access to systems, including those within U.S. critical infrastructure.[2] Recent intrusions targeting programmable logic controllers (PLCs) hardcoded with a four-digit password demonstrate the significant potential for real-world harm caused by manufacturers distributing products with static default passwords. In these attacks, the default password was widely known and publicized on open forums where threat actors are known to mine intelligence for use in breaching U.S. systems. IRGC-affiliated actors easily used the default password to access systems that provide critical services to communities across the country. CISA encourages manufacturers to learn from these compromises by reviewing Principles 1 and 3 of the joint guidance, Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software.

Principle 1: Take ownership of customer security outcomes.

Principle 1 focuses on key security areas manufacturers should invest in to protect public safety and health. These areas include setting default configurations so that products are secure against reasonably foreseeable threats, such as threat actors looking up a default password on the public internet and testing it against internet-exposed devices. For example, instead of including a single default password in every version of a product, manufacturers could instead:

- Provide instance-unique setup passwords with the product,
- Provide time-limited setup passwords that disable themselves when a setup process is complete and require activation of more secure authentication approaches, such as phishing-resistant MFA,[3] or
- Require physical access for initial setup and the specification of instance-unique credentials.

[1] The IRGC is an Iranian military organization that the United States designated as a foreign terrorist organization in 2019.
[2] NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations | CISA
[3] CISA.gov/mfa

Note: CISA understands that these specifics approaches are not viable in some situations due to particular product constraints. However, the key message is for manufacturers to ensure that customers do not bear the security burden.

The goal of this principle is to create **enduring security** for the long-term administration of products starting with the installation process. Manufacturers should not assume that users know they must disable insecure default configurations. Instead, manufacturers should follow the above alternatives or design their own setup flow to secure their products and not put the burden of secure configuration on customers.

Additionally, manufacturers should conduct field tests to understand (1) how their customers deploy products in their unique environments and (2) whether customers are deploying products in unsafe ways. Analysis of these field tests will help bridge the gap between developer expectations and actual customer usage of the product. It will also help identify ways to build the product so customers will be most likely to securely use it—manufacturers should ensure that the easiest route is the secure one. For example, for many products, this route includes manufacturers supporting integration with enterprise identity and access management systems, such as single sign-on (SSO) systems, at no additional cost to the customer.

Principle 3: Build organizational structure and leadership to achieve these goals.

Manufacturers should ensure that business units that own the design, development, and delivery of products and services understand that cybersecurity issues are, at their core, **product and public safety issues** and should be treated as such. Manufacturers should ensure that design and development teams engineer products with security and safety built in by default. Design, development, and delivery teams should prioritize understanding research on how real customers use product configurations and how those configuration choices, in turn, create or mitigate cybersecurity risks. Executive leadership can ensure that feedback on how customers use products meaningfully informs product changes to create safe defaults that reduce risk. Executive leadership should also build the incentive structures within the business—especially at the inception of product design and development—and allocate appropriate resources to their design, development, and delivery teams to enable these outcomes.

Action Item for Software Manufacturers

Although this Secure by Design Alert focuses on avoiding the use of default passwords,[4] it is just one part of a more comprehensive set of secure by design practices. To protect their customers from a wide range of malicious cyber activity, manufacturers should adopt the principles set forth in Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software. Further, CISA urges manufacturers to publish their own secure by design roadmap to demonstrate that they are not simply implementing tactical controls but are strategically rethinking their responsibility in keeping customers safe.

[4] The OWASP Foundation. "Insecure Passwords and Default Credentials." OWASP Top 10 Insider Threats - 2023. July 2023. https://owasp.org/www-project-top-10-insider-threats/docs/2023/INT07_2023-Insecure_Passwords_and_Default_Credentials.