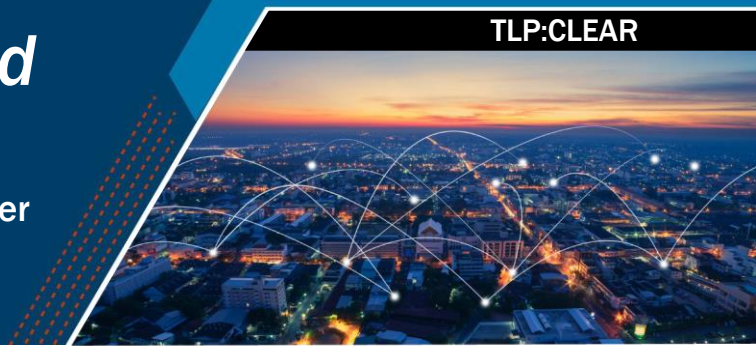
Alerta de seguridad desde el diseño

Cómo los fabricantes pueden proteger a los clientes eliminando las contraseñas predeterminadas



Los agentes cibernéticos malintencionados explotan las contraseñas predeterminadas

Si bien los agentes de amenazas afiliados al Cuerpo de la Guardia Revolucionaria Islámica del Gobierno iraní han sido noticia recientemente al explotar contraseñas predeterminadas, la guía para que los proveedores utilicen alternativas a las contraseñas predeterminadas no es nueva. La CISA y otras entidades en la comunidad de la ciberseguridad han estado emitiendo advertencias similares durante años, pero el daño impuesto a los clientes continúa. Ahora es el momento de que todos los fabricantes de tecnología tomen medidas.

Los agentes cibernéticos malintencionados continúan explotando contraseñas predeterminadas (por ejemplo, "1234", "predeterminado", "contraseña") en sistemas expuestos a Internet para obtener acceso inicial a las organizaciones y moverse lateralmente dentro de ellas. Los agentes de amenazas, incluidos aquellos afiliados al Cuerpo de la Guardia Revolucionaria Islámica (IRGC, por sus siglas en inglés),[1] han logrado comprometer sistemas de infraestructura crítica en los Estados Unidos mediante la explotación de productos de tecnología operativa (OT, por sus siglas en inglés) vendidos por fabricantes con contraseñas configuradas con un valor predeterminado estático. La CISA publica esta alerta, basada en la actividad de amenazas reciente y actual, para instar a todos los fabricantes de tecnología a eliminar las contraseñas predeterminadas en el diseño, el lanzamiento y la actualización de todos los productos. Años de evidencia han demostrado que confiar en que miles de clientes cambien sus contraseñas no es suficiente, y solo la acción concertada de los fabricantes de tecnología abordará de forma adecuada los graves riesgos que enfrentan las organizaciones de infraestructura crítica.

Lecciones por aprender de Seguridad desde el diseño

Un principio fundamental de la seguridad desde el diseño es que los fabricantes creen un comportamiento predeterminado seguro en los productos que ofrecen a los clientes. El uso de contraseñas predeterminadas ampliamente conocidas es inaceptable dado el entorno de amenazas actual. Los estudios de la CISA muestran que el uso de credenciales predeterminadas, como contraseñas, es una de las principales debilidades que los agentes de amenazas explotan para obtener acceso a los sistemas, incluidos aquellos dentro de la infraestructura crítica de EE. UU.[2] Las intrusiones recientes dirigidas a controladores lógicos programables (PLC, por sus siglas en inglés) codificados con una contraseña de cuatro dígitos demuestran el potencial significativo de daño en el mundo real causado por los fabricantes que distribuyen productos con contraseñas predeterminadas estáticas. En estos ataques, la contraseña predeterminada era ampliamente conocida y estaba publicada en foros abiertos, de donde se sabe que los agentes de amenazas extraen información para usarla en vulneraciones de los sistemas estadounidenses. Los agentes afiliados al IRGC utilizaron fácilmente la contraseña predeterminada para acceder a sistemas que brindan servicios críticos a comunidades de todo el país. La CISA anima a los fabricantes a aprender de estos compromisos revisando los Principios 1 y 3 de la guía conjunta, Cambiar el equilibrio del riesgo de la ciberseguridad: principios y enfoques para un software seguro desde el diseño.

Principio 1: Asumir los resultados del cliente en materia de seguridad.

El principio 1 se centra en áreas de seguridad clave en las que los fabricantes deberían invertir para proteger la seguridad y la salud públicas. Estas áreas incluyen establecer configuraciones predeterminadas para que los productos sean seguros contra amenazas razonablemente previsibles, como agentes de amenazas que buscan una contraseña predeterminada en la Internet pública y la prueban en dispositivos expuestos a Internet. Por ejemplo, en lugar de incluir una única contraseña predeterminada en cada versión de un producto, los fabricantes podrían hacer lo siguiente:

- Proporcionar contraseñas de configuración exclusivas para cada instancia con el producto.
- Facilitar contraseñas de configuración de tiempo limitado que se desactiven al finalizar el proceso de configuración y requieran la activación de enfoques de autenticación más seguros, como la MFA resistente al phishing.[3]
- Requerir acceso físico para la configuración inicial y la especificación de credenciales únicas de la instancia.

[1] El IRGC es una organización militar iraní que Estados Unidos designó como organización terrorista extranjera en 2019.
[2] Equipos rojos y azules de la NSA y la CISA comparten los diez errores de configuración más comunes en materia de ciberseguridad | CISA
[3] CISA.gov/mfa

Nota: la CISA entiende que estos enfoques específicos no son viables en algunas situaciones debido a restricciones particulares del producto. Sin embargo, el mensaje clave es que los fabricantes deben garantizar que los clientes no soporten la carga de la seguridad.

El objetivo de este principio es crear **una seguridad duradera** para la administración a largo plazo de los productos a partir del proceso de instalación. Los fabricantes no deben asumir que los usuarios saben que deben desactivar las configuraciones predeterminadas inseguras. En lugar de ello, deberían seguir las alternativas anteriores o diseñar su propio flujo de configuración para proteger sus productos y no dejar la carga de la configuración segura a los clientes.

Además, los fabricantes deberían realizar pruebas de campo para comprender (1) cómo sus clientes implementan los productos en sus entornos únicos y (2) si los clientes están implementando los productos de manera insegura. El análisis de estas pruebas de campo ayudará a cerrar la brecha entre las expectativas de los desarrolladores y el uso real del producto por parte del cliente. También ayudará a identificar formas de construir el producto para que los clientes tengan más probabilidades de usarlo de forma segura; los fabricantes deben asegurarse de que la ruta más fácil sea la segura. Por ejemplo, para muchos productos, esta ruta incluye a los fabricantes que respaldan la integración con sistemas de gestión de acceso e identidad empresarial, como sistemas de inicio de sesión único (SSO, por sus siglas en inglés), sin costo adicional para el cliente.

Principio 3: Construir estructura organizativa y liderazgo para lograr estos objetivos.

Los fabricantes deben asegurarse de que las unidades de negocio que poseen el diseño, el desarrollo y la entrega de productos y servicios comprendan que las cuestiones de ciberseguridad son, en esencia, **cuestiones de seguridad pública y del producto** y deben tratarse como tales. Los fabricantes deben asegurarse de que los equipos de diseño y desarrollo diseñen productos con seguridad y protección incorporadas de forma predeterminada. Los equipos de diseño, desarrollo y entrega deben priorizar la comprensión de las investigaciones sobre cómo los clientes reales utilizan las configuraciones de productos y cómo esas opciones de configuración, a su vez, crean o mitigan riesgos de ciberseguridad. El liderazgo ejecutivo puede garantizar que las valoraciones sobre cómo los clientes usan los productos conformen de manera significativa los cambios en los productos para crear valores predeterminados seguros que reduzcan el riesgo. El liderazgo ejecutivo también debe construir las estructuras de incentivos dentro de la empresa, sobre todo al inicio del diseño y desarrollo del producto, y asignar recursos apropiados a sus equipos de diseño, desarrollo y entrega para posibilitar estos resultados.

Punto de acción para los fabricantes de software

Si bien esta Alerta de seguridad desde el diseño se centra en evitar el uso de contraseñas predeterminadas,[4] es solo una parte de un conjunto más completo de prácticas de seguridad desde el diseño. Para proteger a sus clientes de una amplia gama de actividades cibernéticas maliciosas, los fabricantes deben implementar los principios establecidos en Cambiar el equilibrio del riesgo de la ciberseguridad: principios y enfoques para un software seguro desde el diseño. Además, la CISA insta a los fabricantes a publicar su propia hoja de ruta de seguridad desde el diseño para demostrar que no están simplemente implementando controles tácticos, sino que están repensando de forma estratégica su responsabilidad de mantener seguros a los clientes.

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