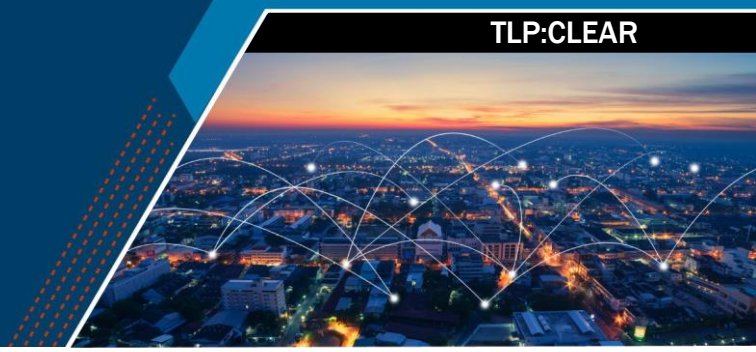
TLP:CLEAR

Alerta de seguridad desde el diseño

Cómo los fabricantes de software pueden proteger las interfaces de gestión web de actividades cibernéticas maliciosas



Actividad cibernética maliciosa contra interfaces de administración web vulnerables

Los agentes cibernéticos maliciosos continúan encontrando y explotando vulnerabilidades en las interfaces de gestión web. En respuesta, los fabricantes de software continúan preguntando por qué los clientes no fortalecen sus productos para evitar este tipo de incidentes.

Lecciones por aprender de Seguridad desde el diseño

"Seguro desde el diseño" significa que los fabricantes de software construyen sus productos de una manera que los proteja razonablemente contra agentes cibernéticos maliciosos que explotan las vulnerabilidades de sus productos. La incorporación de esta medida de mitigación de riesgos, a su vez, reduce la carga de la ciberseguridad sobre los clientes. La explotación de vulnerabilidades en las interfaces de gestión web continúa causando daños importantes a organizaciones de todo el mundo, pero se puede evitar a gran escala. La CISA insta a los fabricantes de software a revisar los principios que se indican a continuación para aprender de la continua actividad cibernética maliciosa contra las interfaces de gestión web.

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

El Principio 1 se centra en áreas clave en las que los fabricantes de software deberían invertir en seguridad: fortalecimiento de las aplicaciones, características de las aplicaciones y configuraciones predeterminadas. Al diseñar estas áreas, los fabricantes de software deben **examinar la configuración predeterminada de sus productos**. Por ejemplo, si se sabe que proteger un sistema de la Internet pública es una buena práctica, no confíe en que los clientes lo hagan. En lugar de ello, es necesario que el **propio producto** aplique las prácticas recomendadas de seguridad. Entre los ejemplos, se incluyen los siguientes:

- Deshabilitar la interfaz web del producto de forma predeterminada e incluir una "guía de flexibilización" que enumera los riesgos (en lenguaje técnico y no técnico) que conlleva realizar cambios en las configuraciones predeterminadasi
- Configurar el producto para que no funcione mientras esté en un estado vulnerable, como cuando el producto está expuesto directamente a Internet.
- Advertir al administrador que cambiar el comportamiento predeterminado puede suponer un riesgo significativo para la organización.

Además, los fabricantes de software deberían realizar pruebas de campo para comprender cómo sus clientes implementan los productos en sus entornos únicos y si están implementando los productos de manera insegura. Esta práctica ayudará a cerrar la brecha entre las expectativas de los desarrolladores y el uso real del producto por parte del cliente. Las pruebas de campo ayudarán a identificar formas de construir el producto para que los clientes lo utilicen de forma segura.

Además, los fabricantes de software deberían exigir de forma sistemática la autenticación en todos sus productos, sobre todo en interfaces críticas como los portales de administrador.

Principio 2: Adoptar métodos radicales de transparencia y rendición de cuentas

Los fabricantes de software deben actuar con transparencia al revelar las vulnerabilidades de sus productos. Para tal fin, los fabricantes deben rastrear la causa subyacente de las vulnerabilidades y asegurarse de que las entradas CVE estén completas e incluyan el campo CWE apropiado que indica la clase de error de codificación que provocó la vulnerabilidad. Esto no solo ayuda a los clientes a comprender y evaluar el riesgo, sino que también permite que otros fabricantes de software aprendan de los errores corregidos en toda la industria.

Por último, los fabricantes de software deberían tratar de identificar (y tomar medidas para eliminar) las clases repetidas de vulnerabilidades en los productos.

Para obtener más información, revise el Cambiar el equilibrio del riesgo de la ciberseguridad: principios y enfoques para un software seguro desde el diseño.

Punto de acción para los fabricantes de software

Para proteger a sus clientes de actividades cibernéticas maliciosas dirigidas a las interfaces de administración web, los fabricantes de software deberían adoptar los principios establecidos en Cambiar el equilibrio del riesgo de la ciberseguridad y publicar su propia hoja de ruta de seguridad desde el diseño que demuestre que no están simplemente implementando controles tácticos, sino que están repensando su papel para mantener seguros a los clientes.

---

[i] Se han detectado múltiples vulnerabilidades explotadas conocidas (KEV, por sus siglas en inglés) que involucran interfaces de administración y, sobre todo, las versiones habilitadas para la web. Por ejemplo, la CISA agregó las siguientes vulnerabilidades al Catálogo de KEV este año: CVE-2023- 20198, CVE-2017-6884, CVE-2023-38035 y CVE-2019-17621, que afectan las interfaces de administración web en los productos Cisco, Zyxel, Ivanti y D-Link, respectivamente.