TLP:CLEAR

Alerta de seguridad desde el diseño

Mejoras en el diseño de seguridad para fabricantes de dispositivos SOHO

Agentes cibernéticos maliciosos que explotan enrutadores SOHO inseguros

Los agentes de amenazas, en particular el grupo Volt Typhoon patrocinado por la República Popular China (PRC, por sus siglas en inglés), están comprometiendo enrutadores de oficina pequeña/oficina en casa (SOHO, por sus siglas en inglés) explotando defectos de software que los fabricantes deben eliminar mediante el diseño y desarrollo de software seguro. En concreto, los agentes de Volt Typhoon están explotando defectos de seguridad en los enrutadores SOHO para usarlos como plataformas de lanzamiento para comprometer aún más las entidades de infraestructura crítica de EE. UU. La CISA y la Oficina Federal de Investigaciones (FBI, por sus siglas en inglés) publican esta alerta basándose en la actividad de amenazas reciente y actual para instar a los fabricantes de enrutadores SOHO a incorporar seguridad en sus productos tecnológicos desde el principio y alentar a todos los clientes de enrutadores SOHO a exigir una mejor seguridad desde el diseño.

Si bien los agentes patrocinados por la República Popular China, incluido el grupo Volt Typhoon, han sido noticia al explotar defectos del software de los enrutadores SOHO, las pautas para que los fabricantes implementen un diseño y desarrollo de software seguro que pueda eliminar estos defectos no son nuevas.

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. “Seguro desde el diseño” significa que los fabricantes diseñan y construyen sus productos de una manera que los proteja de forma razonable contra agentes cibernéticos maliciosos que explotan con éxito los defectos del producto. Incorporar esta medida de mitigación de riesgos desde el principio (comenzando en la fase de diseño y continuando durante el lanzamiento y las actualizaciones) reduce la carga de la ciberseguridad para los clientes y el riesgo para el público.

Los enrutadores SOHO son dispositivos omnipresentes y económicos que conectan a millones de estadounidenses y pequeñas empresas a Internet. Sin embargo, debido a la venta generalizada y el uso posterior de enrutadores SOHO inseguros que carecen de funciones de seguridad básicas, los agentes de amenazas, incluido el grupo Volt Typhoon patrocinado por la República Popular China, están explotando estos dispositivos a gran escala. Además, estos agentes están aprovechando los enrutadores SOHO comprometidos para trasladarse a entidades de infraestructura crítica de EE. UU. y comprometerlas aún más. La creación de productos que carezcan de controles de seguridad adecuados es inaceptable dado el entorno de amenazas actual. Este caso ejemplifica cómo la falta de prácticas seguras desde el diseño puede provocar daños reales tanto a los clientes como, en este caso, a la infraestructura crítica de nuestra nación.

Los fabricantes, a menudo, diseñan y construyen enrutadores SOHO que **carecen de capacidades de actualización automática** e incluyen **una gran cantidad de defectos explotables en las interfaces de administración web**, lo que hace que estos dispositivos sean vulnerables a formas comunes de compromiso. Los fabricantes agravan estos problemas de seguridad al crear dispositivos con interfaces de gestión expuestas a la Internet pública de manera predeterminada, a menudo sin notificar a los clientes sobre esta configuración que suele ser insegura.

Los fabricantes deben diseñar, desarrollar y entregar enrutadores SOHO teniendo en cuenta la seguridad para crear resiliencia del producto frente a amenazas previsibles. La CISA y la FBI animan a los fabricantes a aprender de estos compromisos recientes de Volt Typhoon mediante la revisión de los principios establecidos en Cambiar el equilibrio del riesgo de la ciberseguridad: principios y enfoques para un software seguro desde el diseño. Además, los fabricantes deben revisar y seguir el Informe Interinstitucional 8425 del Instituto Nacional de Estándares y Tecnología (NIST IR, por sus siglas en inglés) sobre la Internet de las cosas (IoT, por sus siglas en inglés) y el borrador preliminar del Perfil de ciberseguridad de la IoT para enrutadores de consumo del NIST.

A 31 de enero de 2024

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 a sus clientes y al público. Estas áreas incluyen la configuración predeterminada que protege los dispositivos contra amenazas previsibles. Por ejemplo, los fabricantes de enrutadores SOHO deberían considerar lo siguiente:

- Implementar actualizaciones de software automatizadas y firmadas para abordar vulnerabilidades de seguridad, idealmente sin ninguna intervención del usuario. (Consulte NIST IR 8425 "Actualización de software").
- Colocar la interfaz de administración web en los puertos del lado LAN para proteger contra exposición vulnerable.
- Mejorar la seguridad del sistema de interfaz de gestión para permitir un uso seguro cuando se expone a Internet pública, incluso trabajando para eliminar clases enteras de vulnerabilidad del producto.
- Establecer valores predeterminados seguros que los clientes deben anular de forma manual e incluir una redacción lo bastante contundente para disuadirlos de hacerlo, a menos que hayan implementado controles compensatorios. (Consulte NIST IR 8425 "Configuración del producto").

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

Los fabricantes deben actuar con transparencia al revelar las vulnerabilidades de sus productos. Para tal fin, los fabricantes deberían rastrear las clases de vulnerabilidad asociadas con sus enrutadores SOHO y revelarlas a sus clientes a través del programa de CVE. Los fabricantes deben asegurarse de que sus registros de CVE sean correctos y completos. Es especialmente importante que los fabricantes proporcionen una CWE precisa para que la industria pueda rastrear clases de defectos de software, no solo CVE individuales, y los clientes puedan comprender áreas en las que las prácticas de desarrollo de un proveedor determinado pueden requerir mejoras.[i] También deben identificar y documentar las causas fundamentales de esas vulnerabilidades y declarar como objetivo comercial trabajar para eliminar clases enteras de vulnerabilidades.

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

Así como los ejecutivos de fabricación de software y hardware se preocupan por el costo, también deberían priorizar la seguridad de sus productos. Los líderes deben considerar el panorama completo: que los clientes, nuestra economía y nuestra seguridad nacional actualmente soportan el peso de las decisiones comerciales de no incorporar seguridad a sus productos. Además, orientar la empresa hacia el desarrollo de software seguro desde el diseño puede reducir los costos financieros y de productividad, así como la complejidad. Los líderes deben realizar las inversiones apropiadas y desarrollar las estructuras de incentivos correctas que promuevan la seguridad como un objetivo comercial declarado.

Punto de acción para los fabricantes de software

Si bien esta Alerta de seguridad desde el diseño se centra en cómo los fabricantes de SOHO pueden proporcionar dispositivos seguros, 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 por completo los principios y las prácticas abordados en esta alerta mediante la revisión de Cambiar el equilibrio del riesgo de la ciberseguridad: principios y enfoques para un software seguro desde el diseño. Además, la CISA instan 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.

[i] La clasificación de enumeración de debilidades comunes (CWE, por sus siglas en inglés) identifica clases de debilidades de software y hardware (incluidas vulnerabilidades y defectos); la clasificación de vulnerabilidades y exposiciones comunes (CVE, por sus siglas en inglés) identifica y etiqueta vulnerabilidades únicas en productos de software y hardware específicos.