La Agencia de Seguridad e Infraestructura de Ciberseguridad de Estados Unidos (CISA), advirtió sobre vulnerabilidades críticas en una biblioteca de software TCP/IP de bajo nivel, desarrollada por Treck, que en caso de utilizarse como arma, podría permitir a los atacantes remotos ejecutar comandos arbitrarios y montar ataques de denegación de servicio (DoS).

Las cuatro vulnerabilidades afectan la pila Treck TCP/IP versión 6.0.1.67 y anteriores, y fueron informadas a la compañía por Intel. Dos de las fallas están clasificadas como críticas en severidad.

La pila TCP/IP integrada de Treck se implementa en todo el mundo en sistemas de fabricación, tecnología de la información, atención médica y transporte.

El más grave de ellos es una vulnerabilidad de desbordamiento de búfer basada en montones (CVE-2020-25066) en el componente Treck HTTP Server, que podría permitir que un adversario bloquee o reinicie el dispositivo de destino e incluso ejecute código remoto. Tiene una puntuación CVSS de 9.8 sobre 10.

La segunda vulnerabilidad es una escritura fuera de límites en el componente IPv6 (CVE-2020-27337, CVSS 9.1) que podría ser aprovechada por un usuario no autenticado para causar una condición DoS a través del acceso a la red.

Otras dos vulnerabilidades se refieren a una lectura fuera de los límites en el componente IPv6 (CVE-2020-27338, CVSS 5.9), que podría ser aprovechada por un atacante no autenticado para causar ataques DoS y una validación de entrada incorrecta en el mismo módulo (CVE-2020-27336, CVSS 3.7), que podría resultar en una lectura fuera de límites de hasta tres bytes a través del acceso a la red.

Treck recomienda a los usuarios que actualicen la pila a la versión 6.0.1.68 para solucionar los defectos. En los casos en que no se puedan aplicar los últimos parches, se recomienda que se implementen reglas de firewall para filtrar los paquetes que contienen una longitud de contenido negativa en el encabezado HTTP.

La revelación de nuevas fallas en la pila TCP/IP de Treck se produce seis meses después de que la empresa israelí de ciberseguridad JSOF descubrió 19 vulnerabilidades en la biblioteca de software, denominada Ripple20, que podría hacer posible que los atacantes obtengan un control completo sobre los dispositivos IoT específicos sin requerir la autenticación del usuario.

Por otro lado, a inicios de este mes, los investigadores de Forescout revelaron 33 vulnerabilidades, denominadas de forma colectiva como AMNESIA:33, que afectan a las pilas de protocolos TCP/IP de código abierto que podrían ser abusadas por un mal actor para hacerse cargo de un sistema vulnerable.

Debido a la compleja cadena de suministro de IoT involucrada, la compañía ha lanzado una nueva herramienta de detección llamada project-memoria-detector para identificar si un dispositivo de red objetivo ejecuta una pila TCP/IP vulnerable en un entorno de laboratorio.