Vulnerabilidades en pilas TCP/IP de Treck

BCSC-VULNERABILIDADES_PILAS_TCP_IP_TRECK

TLP:WHITE

www.basquecybersecurity.eus

Diciembre 2020

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

SOBRE EL BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

RESUMEN EJECUTIVO

Se han hecho públicas cuatro vulnerabilidades, 2 de ellas críticas, en una librería de software **TCP/IP** de bajo nivel desarrollada por **Treck,** que utilizada de forma malintencionada podría permitir a un atacante remoto ejecutar código o provocar una denegación de servicio (DoS). La pila TCP/IP integrada de Treck se encuentra implementada en todo el mundo principalmente en sistemas de **fabricación**, **tecnologías de la información** y sectores críticos como la **salud** y el **transporte**.

El propio fabricante Treck ha recomendado actualizar la pila a la versión **6.0.1.68** para solucionar estos defectos y, en caso de no ser posible aplicar los últimos parches, existen diversas medidas de mitigación para reducir la exposición y el riesgo a ataques que aprovechen estas vulnerabilidades.

La publicación de estos nuevos fallos en la pila TCP/IP de Treck se produce seis meses después del reporte, por parte de la compañía de ciberseguridad JSOF, de 19 vulnerabilidades (Ripple20) en la misma librería de software de Treck que permiten conseguir un control completo sobre dispositivos IoT específicos sin requerir la interacción de un usuario. Además, a principios de este mes de diciembre, investigadores de la firma Forescout revelaron 33 vulnerabilidades, denominadas colectivamente AMNESIA:33, que también afectan a pilas de protocolos TCP/IP de código abierto y que podrían explotarse con el fin de tomar el control de sistemas vulnerables.

Para facilitar la detección de dispositivos vulnerables y ante la compleja cadena de suministro de IoT involucrada, Forescout ha lanzado una nueva herramienta de detección llamada "***project-memoria-detector***" que identifica si un dispositivo de red objetivo ejecuta una pila TCP/IP vulnerable.

ANÁLISIS TÉCNICO

La pila **TCP/IP** de **Treck** es una librería de software TCP/IP de bajo nivel diseñada específicamente para **sistemas integrados** ampliamente utilizada en sectores críticos de **fabricación, TI, sanidad y transporte**. Recientemente se han hecho públicas cuatro nuevas vulnerabilidades de las que dos de ellas han sido calificadas como de gravedad crítica.

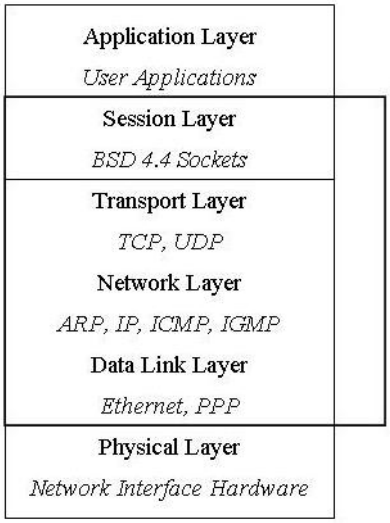

Ilustración 1. Treck TCP/IP stack

El error más grave se trata de una **vulnerabilidad de desbordamiento de búfer** en el **componente Treck** del servidor **HTTP** que podría permitir a un atacante reiniciar dispositivos e incluso ejecutar código de forma remota. La vulnerabilidad ha sido identificada con el **CVE-2020-25066** y con un score de **9.8** según la escala **CVSSv3.1**.

El segundo fallo más grave es una **vulnerabilidad de escritura fuera de límites** en el **componente IPv6** que podría ser explotada por un usuario no autenticado para causar una condición de denegación de servicio (DoS) mediante el acceso a una red determinada. La vulnerabilidad ha sido identificada con el **CVE-2020-27337** y con un score de **9.1** según la escala **CVSSv3.1**.

Las dos vulnerabilidades restantes y menos graves consisten también en errores que permiten la **lectura fuera de límites en el componente IPv6** (CVE-2020-27338, score de 5.9 CVSSv3.1) que podría ser aprovechada por un atacante no autenticado para causar una denegación de servicio y un fallo de **validación de entrada inadecuada en el mismo componente** (CVE-2020-27336, score de 3.7 CVSSv3.1) que podría resultar en una lectura fuera de límites de hasta tres bytes mediante el acceso a una red determinada.

No obstante, se debe tener en cuenta que son vulnerabilidades que requieren de **altas habilidades para su explotación** y, por el momento, no se conocen ataques conocidos de forma pública, exploits disponibles o pruebas de concepto específicas sobre ellas.

MITIGACIÓN / SOLUCIÓN

La propia compañía **Treck** ha recomendado a los usuarios que actualicen la pila a la versión **6.0.1.68 o posterior** con el fin de solucionar estas vulnerabilidades. En los casos en los que no sea posible aplicar los parches, se recomienda **implementar reglas de firewall** para filtrar los paquetes que contengan una **longitud de contenido negativa en el encabezado HTTP**. Para obtener los parches, es necesario enviar un correo electrónico a security@treck.com

Tal y como ya se ha mencionado anteriormente, para facilitar la detección de dispositivos vulnerables y ante la compleja cadena de suministro de IoT involucrada, Forescout ha lanzado una nueva herramienta de detección llamada "***project-memoria-detector***" que identifica si un dispositivo de red objetivo ejecuta una pila TCP/IP vulnerable.

Además, con el fin de reducir al mínimo el riesgo de explotación de estas vulnerabilidades, se recomienda adoptar las siguientes medidas:

- Minimizar la exposición a la red de todos los dispositivos y/o sistemas de control y asegurarse de que no sean accesibles desde Internet.
- Localizar las redes de sistemas de control y los dispositivos remotos detrás de los firewalls y aislarlos de la red de la empresa.
- En caso de necesitar accesos remotos, utilizar métodos seguros, como las redes privadas virtuales (VPN), teniendo en cuenta que estas redes pueden tener vulnerabilidades y deben actualizarse a la versión más reciente disponible.

Adicionalmente, se debe tener en cuenta que es necesario realizar un análisis de impacto y una evaluación de riesgos adecuados antes de desplegar estas medidas defensivas.

Cabe destacar que el US Cybersecurity Infrastructure and Security Agency (CISA) tiene disponible una guía de prácticas recomendadas de seguridad en los sistemas de control. Estas prácticas recomendadas están disponibles para su lectura y descarga, incluyendo mejoras en la ciberseguridad de los **Sistemas de Control Industrial** en base a profundas estrategias de defensa.

REFERENCIAS ADICIONALES

- Treck - VU#114986 and ICS-VU-870237 – Affects versions 6.0.1.67 and earlier
- ICS Advisory (ICSA-20-353-01) - Treck TCP/IP Stack
- Industrial Control Systems - Recommended Practices

Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?