El Departamento de Seguridad Nacional y CISA ICS-CERT, advirtieron sobre un problema de seguridad crítica de asesoramiento, que involucra 19 nuevas vulnerabilidades que afectan a mil millones de dispositivos conectados a Internet fabricados por más de 500 proveedores en todo el mundo.

Nombrado como Ripple20, el conjunto de 19 vulnerabilidades reside en una biblioteca de software TCP/IP de bajo nivel desarrollada por Treck, que de estar armada, podría permitir a los atacantes remotos tener un control completo sobre los dispositivos objetivo, sin requerir ninguna interacción del usuario.

JSOF, compañía israelí de seguridad cibernética que descubrió los defectos, afirma que los dispositivos afectados se utilizan en diversas industrias, desde dispositivos domésticos y de consumo, hasta médicos, centros de datos, empresas, telecomunicaciones, petróleo, gas, energía nuclear, transporte y muchos más.

> *«Solo algunos ejemplos: los datos pueden ser robados de una impresora, el comportamiento de una bomba de infusión puede cambiar, o los dispositivos de control industrial pueden funcionar mal. Un atacante podría ocultar el código malicioso dentro de los dispositivos integrados durante años»,* dijeron los investigadores.
>
> *«Una de las vulnerabilidades podría permitir la entrada desde el exterior a los límites de la red. Esto es solo una pequeña muestra de los riesgos potenciales»,* agregaron.

Existen cuatro vulnerabilidades críticas en la pila Treck TCP/IP, con puntajes CVSS superiores a 9, lo que podría permitir a los hackers ejecutar código arbitrario en dispositivos de forma remota, y un error crítico afecta el protocolo DNS.

> *«Las otras 15 vulnerabilidades están en diversos grados de severidad con un puntaje CVSS que varía de 3.1 8.2, y efectos que van desde la denegación de servicio hasta la posible ejecución remota de código»,* dice el informe.

Treck o los fabricantes de dispositivos repararon algunas fallas de Ripple20 a lo largo de los años debido a cambios en el código y la configuración de la pila, y por la misma razón, muchas de las fallas también tienen variantes que aparentemente no se corregirán en el corto plazo hasta que los proveedores realicen una evaluación integral de riesgos.

- CVE-2020-11896 (CVSS v3 base score 10): manejo inadecuado de la inconsistencia del parámetro de longitud en el componente IPv4/UDP cuando se maneja un paquete enviado por un atacante de red no autorizado. Esta vulnerabilidad puede provocar la ejecución remota de código.
- CVE-2020-11897 (CVSS v3 base score 10): manejo inadecuado de la inconsistencia del parámetro de longitud en el componente IPv6 cuando se maneja un paquete enviado por un atacante de red no autorizado. Esta vulnerabilidad podría resultar en una posible escritura fuera de los límites.
- CVE-2020-11898 (CVSS v3 base score 9.8): manejo inadecuado de la inconsistencia de los parámetros de longitud en el componente IPv4/ICMPv4 cuando se maneja un paquete enviado por un atacante de red no autorizado. Esta vulnerabilidad puede provocar la exposición de información confidencial.
- CVE-2020-11899 (CVSS v3 9.8): validación de entrada incorrecta en el componente IPv6 cuando se maneja un paquete enviado por un atacante de red no autorizado. Esta vulnerabilidad puede permitir la exposición de información sensible.
- CVE-2020-11900 (CVSS v3 9.3): posible doble libre en el componente de túnel IPv4 cuando se maneja un paquete enviado por un atacante de red. Esta vulnerabilidad puede provocar la ejecución remota de código.
- CVE-2020-11901 (CVSS v3 9.0): validación de entrada incorrecta en el componente de resolución DNS cuando se maneja un paquete enviado por un atacante de red no autorizado. Esta vulnerabilidad puede provocar la ejecución remota de código.

Se puede encontrar más detalles para el resto de las vulnerabilidades en un aviso publicado por el gobierno de Estados Unidos.

Los investigadores de seguridad cibernética de JSOF, informaron responsablemente sus hallazgos a la compañía Treck, que luego reparó la mayoría de las vulnerabilidades mediante una versión de pila TCP/IP 6.0.1.67 o superior.

Los investigadores también se comunicaron con más de 500 vendedores de semiconductores y fabricantes de dispositivos afectados, incluidos HP, Schneider Electric, Intel, Rockwell Automation, Caterpillar, Baxter y Quadros, muchos de los cuales reconocieron la falla y el resto siguen evaluando sus productos antes de hacerlo público.

> *«La divulgación se pospuso dos veces después de que algunos de los proveedores participantes solicitaron más tiempo, y algunos de los vendedores expresaron demoras relacionadas con COVID-19. Por consideración a estas compañías, el período de tiempo se extendió de 90 a más de 120 días. Aún así, algunas de las compañías participantes se volvieron difíciles de tratar, ya que hicieron demandas adicionales, y algunas, desde nuestra perspectiva, parecían mucho más preocupadas por la imagen de su marca que por parchear las vulnerabilidades»*, dijeron los investigadores.

Debido a que millones de dispositivos no recibirán actualizaciones de parches de seguridad para abordar las vulnerabilidades de Ripple20 en el corto plazo, los investigadores y la ICS-CERT recomendaron a los consumidores lo siguiente:

- Minimizar la exposición de la red para todos los dispositivos y/o sistemas de control y asegurarse de que no sean accesibles desde Internet.
- Ubicar las redes del sistema de control y los dispositivos remotos detrás de los firewall y aislarlos de la red empresarial.

Además, también se recomienda utilizar redes privadas virtuales para conectar de forma

segura sus dispositivos a servicios basados en la nube por medio de Internet.

En su asesoría, CISA también pidió a las organizaciones afectadas que realicen un análisis de impacto y una evaluación de riesgos adecuados antes de implementar medidas defensivas.