Los investigadores de seguridad descubrieron casi 12 vulnerabilidades de día cero en VxWorks, uno de los sistemas operativos en tiempo real (RTOS) más utilizados para dispositivos integrados que alimenta a más de 2 mil millones de dispositivos en la industria aeroespacial, de defensa, industrial, médica, automotriz y de consumo, redes y otras industrias críticas.

Según un nuevo informe de investigadores de Armis, las vulnerabilidades se denominan como URGENT/11, ya que son 11 en total, de las cuales, seis son de gravedad crítica y conducen a ataques cibernéticos *«devastadores».*

Armis Labs es la misma compañía de seguridad de IoT que descubrió anteriormente las vulnerabilidades de BlueBorne en el protocolo Bluetooth que afectaron a más de 5.3 mil millones de dispositivos, con sistemas Android, iOS, Windows, Linux y hasta equipos referentes a Internet de las Cosas (IoT).

Estas vulnerabilidades podrían permitir a los hackers remotos eludir las soluciones de seguridad tradicionales y tomar el control total sobre los dispositivos afectados o *«causar interrupciones en una escala similar a la resultante de la vulnerabilidad EternalBluet»,* sin requerir ninguna interacción del usuario.

Es probable que muy pocos hayan escuchado sobre este sistema operativo, pero Wind River VxWorks se está utilizando para ejecutar muchas cosas cotidianas de Internet, como su cámara web, conmutadores de red, enrutadores, firewalls, teléfonos VOIP, impresoras y productos de videoconferencia, así como semáforos.

Además de esto, VxWorks también está siendo utilizado por sistemas de misión crítica que incluyen SCADA, trenes, ascensores y controladores industriales, monitores de pacientes, máquinas de MRI, módems satelitales, sistemas WiFi en vuelo e incluso los Rovers Mars.

URGENT/11 – Vulnerabilidades en VxWorks RTOS

Las vulnerabilidades reportadas residen en la pila de red IPnet TCP/IP del RTOS que se

incluyó en VxWorks desde su versión 6.5, aparentemente dejando a todas las versiones de VxWorks lanzadas en los últimos 13 años vulnerables a los ataques de control de dispositivos.

Las 6 vulnerabilidades críticas permiten a los atacantes desencadenar ataques de ejecución remota de código (RCE), y las fallas que quedan pueden provocar la denegación de servicio, las fugas de información o las fallas lógicas.

Fallos críticos de ejecución remota de código

- Desbordamiento de pila en el análisis de las operaciones de IPv4 (CVE-2019-12256)
- Cuatro vulnerabilidades de corrupción de memoria derivadas del manejo erróneo del campo del puntero urgente de TCP (CVE-2019-12255, CVE-2019-12260, CVE-2019-12261, CVE-2019-12263)
- Desbordamiento de pila de DHCP Offer/ACK parsing, en ipdhcp (CVE-2019-12257)

DoS, Fuga de información y fallas lógicas

- Conexión TCP DoS por medio de opciones TCP mal formadas (CVE-2019-12258)
- Manejo de respuestas ARP inversas no solicitadas (falla lógica) (CVE-2019-12262)
- Defecto lógico en la asignación de IPv4 por el cliente DHCP ipdhcp (CVE-2019-12264)
- DoS a través de referencia NULL en el análisis IGMP (CVE-2019-12259)
- Fuga de información de IGMP a través del informe de membresía específico de IGMPv3 (CVE-2019-12265)

Todas estas vulnerabilidades pueden ser explotadas por un atacante remoto no autenticado simplemente al enviar un paquete TCP especialmente diseñado a un dispositivo afectado sin requerir ninguna interacción del usuario o información previa con respecto al dispositivo objetivo.

Sin embargo, cada versión de VxWorks desde la versión 6.5 no es vulnerables a las 11 fallas, pero al menos una falla crítica de RCE afecta a cada versión del sistema operativo en tiempo

real.

> *«VxWorks incluye algunas mitigaciones opcionales que podrían hacer que algunas de las vulnerabilidades URGENT/11 sean más difíciles de explotar, pero los fabricantes de dispositivos rara vez utilizan estas mitigaciones»*, dicen los investigadores.

Los investigadores de Armis creen que los defectos de URGENT/11 podrían afectar también a los dispositivos que utilizan otros sistemas operativos en tiempo real, ya que IPnet se utilizó en otros sistemas operativos antes de su adquisición por VxWorks en 2006.

¿Cómo pueden los atacantes remotos explotar los defectos de VxWorks?

La explotación de las vulnerabilidades de IPnet de VxWorks también depende de la ubicación de un atacante y el dispositivo vulnerable objetivo, después de todo, los paquetes de red del atacante deberían llegar al sistema vulnerable.

Según los investigadores, la superficie de amenaza de las fallas URGENT/11 se puede dividir en 3 escenarios de ataque, como se observa a continuación:

Escenario 1: Ataque a las defensas de la red

Como VxWorks también alimenta dispositivos de red y de seguridad, como conmutadores, enrutadores y cortafuegos a los que generalmente se puede acceder por medio de Internet pública, un atacante remoto puede lanzar un ataque directo contra estos dispositivos, tomando el control completo sobre ellos, y posteriormente, por las redes internas.

Por ejemplo, existen más de 775,000 firewalls de SonicWall conectados a Internet en este

momento, que ejecutan VxWorks RTOS, según el motor de búsqueda Shodan.

Escenario 2: Ataque desde fuera de la red sin pasar por la seguridad

Además de apuntar a dispositivos conectados a Internet, un atacante también puede intentar apuntar a dispositivos IoT que no están directamente conectados a Internet pero que se comunican con su aplicación basada en la nube protegida por un firewall o una solución NAT.

Según los investigadores, un atacante potencial puede utilizar el malware de cambio de DNS o ataques de hombre en el medio para interceptar la conexión TCP de un dispositivo objetivo a la nube y lanzar un ataque de ejecución de código remoto.

Escenario 3: Ataques desde dentro de la red

En este escenario, un atacante que ya se posicionó dentro de la red como resultado de un ataque anterior puede lanzar ataques contra dispositivos VxWorks afectados simultáneamente, incluso cuando no tienen conexión directa a Internet.

> *«Las vulnerabilidades en estos dispositivos no administrados y de IoT se pueden aprovechar para manipular datos, alterar los equipos del mundo físico y poner en riesgo la vida de las personas»,* dijo Yevgeny Dibrov, CEO y cofundador de Armis.
>
> *«Un controlador industrial comprometido podría cerrar una fábrica, y un monitor de paciente con tecnología de punta podría tener un efecto de amenaza para la vida. Según el mejor conocimiento de ambas compañías, no hay indicios de que se hayan explotado las vulnerabilidades URGENT/11»*, agregó.

Sin embargo, los investigadores también confirmaron que estas vulnerabilidades no afectan otras variantes de VxWorks diseñadas para la certificación, como VxWorks 653 y VxWorks Cert Edition.

Armis informó estas vulnerabilidades a Wind River Systems de forma responsable, y la compañía ya notificó a varios fabricantes de dispositivos y lanzó parches de seguridad para abordar las vulnerabilidades el mes pasado.

Mientras tanto, los proveedores de productos afectados también están en proceso de lanzar parches para sus clientes, lo que los investigadores creen que tomará tiempo y será difícil, como suele ser el caso cuando se trata de IoT y actualizaciones de infraestructura crítica. SonicWall y Xerox ya lanzaron parches para sus dispositivos de firewall e impresoras.