Un investigador de seguridad cibernética reveló hoy los detalles técnicos y prueba de concepto de una vulnerabilidad crítica de ejecución remota de código que afecta a OpenWrt, un sistema operativo basado en Liux ampliamente utilizado para enrutadores, puertas de enlace residenciales y otros dispositivos integrados que enrutan tráfico de red.

La vulnerabilidad, rastreada como CVE-2020-7982, reside en el administrador de paquetes OPKG de OpenWrt que existe en la forma en que realiza la verificación de integridad de los paquetes descargados utilizando las sumas de verificación SHA-256 integradas en el índice de repositorio firmado.

Al invocar el comando *'opkg install'* en el sistema de la víctima, la vulnerabilidad podría permitir que un atacante remoto en el medio puede interceptar la comunicación de un dispositivo objetivo para ejecutar código arbitrario engañando al sistema para que instale un paquete malicioso o actualización de software sin verificación.

De ser explotada con éxito, un atacante remoto podría obtener un control completo sobre el dispositivo de red OpenWrt objetivo, y posteriormente, sobre el tráfico de red que administra.

La vulnerabilidad de tres años fue descubierta a inicios de este año por Guido Vranken, de la compañía de software ForAllSecure, quien luego lo informó de forma responsable al equipo de desarrollo de OpenWrt.

En una entrada de blog de hoy, Vranken explicó que cuando una suma de verificación contiene espacios iniciales, OPKG en las versiones vulnerables de OpenWrt omite verificar la integridad del paquete descargado y sigue con la tarea de instalación.

> *«Debido al hecho de que OPKG en OpenWrt se ejecuta como root y tiene acceso de escritura a todo el sistema de archivo, podría inyectarse código arbitrario mediante paquetes .ipk falsificados con una carga maliciosas»,* dijo el equipo de OpenWrt.

La explotación remota de esta vulnerabilidad es posible debido al hecho de que la integridad en los mecanismos de instalación de software basados en Linux depende de la firma digital de archivos mientras se descargan archivos por medio de una conexión HTTP insegura.

Además, para explotar la vulnerabilidad, los atacantes también deben servir un paquete malicioso con un tamaño igual al especificado en la lista de paquetes en downloads.openwrt.org.

Según el equipo del proyecto, las versiones de OpenWrt 18.06.0 a 18.06.6 y 19.07.0, así como LEDE 17.01.0 a 17.01.7, se ven afectadas.

> *«Como una solución provisional, OpenWrt eliminó el espacio en el SHA256sum de la lista de paquetes poco después de informar el error. Sin embargo, esta no es una solución adecuada a largo plazo porque un atacante simplemente puede proporcionar una lista de paquetes más antigua que fue firmada por los mantenedores de OpenWrt»,* dijo Vranken.

Para solucionar el problema, se recomienda a los usuarios afectados que actualicen el firmware de su dispositivo a las últimas versiones de OpenWrt 18.06.7 y 19.07.1, que se lanzaron el mes pasado.