Los investigadores de seguridad cibernética descubrieron vulnerabilidades en una implementación de software del Protocolo de Puerta de Enlace Fronteriza (BGP), que podría armarse para lograr una condición de denegación de servicio (DoS) en pares BGP vulnerables.

Las tres vulnerabilidades residen en la versión 8.4 de FRRouting, un popular conjunto de protocolos de enrutamiento de Internet de código abierto para plataformas Linux y Unix. Actualmente lo utilizan varios proveedores como NVIDIA Cumulus, DENT y SONiC, lo que plantea riesgos en la cadena de suministro.

El descubrimiento es el resultado de un análisis de siete implementaciones distintas de BGP realizadas por Forescout Vedere Labs: FRRouting, BIRD, OpenBGPd, Mikrotik RouterOS, Juniper JunOS, Cisco iOS y Arista EOS.

BGP es un protocolo de puerta de enlace diseñado para intercambiar información de enrutamiento y accesibilidad entre sistemas autónomos. Se usa para encontrar las rutas más eficientes para entregar tráfico de Internet.

La lista de vulnerabilidades es la siguiente:

- CVE-2022-40302 (puntaje CVSS: 6.5): Lectura fuera de los límites al procesar un mensaje BGP OPEN con formato incorrecto con una opción de longitud de parámetros opcionales extendidos.
- CVE-2022-40318 (puntaje CVSS: 6.5): Lectura fuera de los límites al procesar un mensaje BGP OPEN con formato incorrecto con una opción de longitud de parámetros opciones extendidos.
- CVE-2022-43681 (puntaje CVSS: 6.5): Lectura fuera de los límites al procesar un mensaje BGP OPEN con formato incorrecto que termina abruptamente en el octeto de longitud de opción.

Los problemas *«podrían ser explotados por atacantes para lograr una condición DoS en pares BGP vulnerables, eliminando así todas las sesiones BGP y tablas de enrutamiento y haciendo*

que el par no responda», dijo la compañía en un informe.

> *«La condición DoS puede prolongarse indefinidamente al enviar repetidamente paquetes con formato incorrecto. La principal causa raíz es el mismo patrón de código vulnerable copiado en varias funciones relacionadas con distintas etapas de análisis de mensaje ABIERTOS».*

Un atacante podría falsificar una dirección IP válida de un par BGP confiable o explotar otras vulnerabilidades y configuraciones incorrectas para comprometer a un par legítimo y después emitir un mensaje BGP OPEN no solicitado especialmente diseñado.

Esto se logra aprovechando el hecho de que *«FRRouting comienza a procesar mensajes ABIERTOS (por ejemplo, desencapsulando parámetros opcionales) antes de que tenga la oportunidad de verificar el identificador BGP y los campos ASN del enrutador de origen».*

Forescout también ha puesto a disposición una herramienta de código abierto llamada bgp_boofuzzer que permite a las organizaciones probar la seguridad de las suites BGP usadas internamente, así como encontrar nuevas vulnerabilidades en las implementaciones de BGP.

> *«Las implementaciones modernas de BGP todavía tienen frutos fáciles de los que los atacantes pueden abusar. Para mitigar el riesgo de implementaciones BGP vulnerables, la mejor recomendación es parchear los dispositivos de infraestructura de red con la mayor frecuencia posible»,* dijo Forescout.

Los hallazgos se producen semanas después de que ESET descubriera que los routers de segunda mano usados anteriormente en entornos de redes comerciales albergaban datos

confidenciales, incluidas las credenciales corporativas, detalles de VPN, claves criptográficas y otra información vital del cliente.

> *«En las manos equivocadas, los datos obtenidos de los dispositivos, incluyendo los datos de los clientes, las claves de auteticación de enrutador a enrutador, las listas de aplicaciones y mucho más, son suficientes para lanzar un ataque cibernético»*, dijo la compañía de seguridad eslovaca.