Después de unos 10 días de que la empresa de seguridad de aplicaciones F5 Networks lanzara parches para vulnerabilidades críticas en sus productos BIG-IP y BIG-IQ, los atacantes comenzaron a escanear en masa de forma oportunista y apuntar a dispositivos de red expuestos y sin parches para ingresar a redes empresariales.

La noticia de la explotación en la naturaleza llega inmediatamente después de un código de explotación de prueba de concepto que apareció en línea a inicios de la semana mediante ingeniería inversa el parche de software Java en BIG-IP. Se dice que las exploraciones masivas se han disparado desde el 18 de marzo.

Las vulnerabilidades afectan a las versiones 11.6 o 12.x y más recientes de BIG-IP, con una ejecución de código remoto crítico (CVE-2021-22986) que también afecta las versiones 6.x y 7.x de BIG-IQ.

CVE-2021-22986, con puntuación CVSS de 9.8, se caracteriza por el hecho de que es una vulnerabilidad de ejecución remota de comandos no autenticada que afecta a la interfaz REST de iControl, lo que permite a un atacante ejecutar comandos arbitrarios del sistema, crear o eliminar archivos y deshabilitar servicios sin necesidad de cualquier autenticación.

La explotación exitosa de estas vulnerabilidades podría conducir a un compromiso total de los sistemas susceptibles, incluyendo la posibilidad de ejecución remota de código, así como desencadenar un desbordamiento de búfer, lo que provocaría un ataque de denegación de servicio (DoS).

Aunque F5 afirmó que no estaba al tanto de ninguna explotación pública de estos problemas el 10 de marzo, los investigadores del Grupo NCC, dijeron que ahora encontraron evidencia de *«explotación de cadena completa de las vulnerabilidades de F5 BIG-IP/BIG-IQ iControl REST API CVE-2021-22986»* a raíz de múltiples intentos de explotación contra su infraestructura honeypot.

Además, el equipo de inteligencia de amenazas de la Unidad 42 de Palo Alto Networks dijo que encontró intentos de explotación de CVE-2021-22986 para instalar una variante de la

botnet Mirai, pero no está claro si los ataques tuvieron éxito.

Debido a la popularidad de BIG-IP/BIG-IQ en las redes corporativas y gubernamentales, no debería sorprender que esta sea la segunda vez en un año que los dispositivos F5 se convierten en un objetivo lucrativo para la explotación.

En julio pasado, la compañía abordó una falla crítica similar (CVE-2020-5902), después de la cual fue abusada por grupos de hacking patrocinados por el estado iraní y chino, lo que llevó a la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) a emitir una alerta advirtiendo sobre una *«amplia actividad de escaneo para detectar la presencia de la vulnerabilidad en los departamentos y agencias federales».*

> *«La conclusión es que las fallas afectan a todos los clientes e instancias de BIG-IP y BIG-IQ, instamos a todos los clientes a actualizar sus implementaciones de BIG-IP y BIG-IQ a las versiones fijas lo antes posible»,* dijo Kara Sprague, vicepresidente senior de F5.