F5 Networks, uno de los mayores proveedores a nivel mundial de equipos de redes empresariales, publicó un aviso de seguridad esta semana, en el que advierte a sus clientes que corrijan una falla de seguridad peligrosa tiene alta probabilidad de explotarse.

La vulnerabilidad afecta el producto BIG-IP de la compañía. Estos son dispositivos de red multipropósito que pueden funcionar como sistemas de configuración de tráfico web, equilibradores de carga, firewalls, puertas de acceso, limitadores de velocidad o middleware SSL.

BIP-IP es uno de los productos de red más populares en uso. Se utiliza en redes gubernamentales de todo el mundo, en redes de proveedores de servicios de Internet, en centros de datos de computación en la nube y redes empresariales en general.

F5 dijo en su sitio web que sus dispositivos BIG-IP se utilizan en las redes de 48 compañías incluidas en la lista Fortune 50.

Mikhail Klyuchnikov, investigador de seguridad de Positive Technologies, encontró la vulnerabilidad rastreada como CVE-2020-5902 y la notificó en privado a F5.

Se trata de una vulnerabilidad de ejecución remota de código en la interfaz de administración de BIG-IP, conocida como TMUI (Interfaz de Usuario de Administración de Tráfico).

Los atacantes pueden explotar el error en Internet para obtener acceso al componente TMUI, que se ejecuta sobre un servidor Tomcat en el sistema operativo basado en Linux de BIG-IP.

Los hackers no necesitan credenciales válidas para atacar los dispositivos, y en caso de una explotación exitosa, podrían ejecutar comandos arbitrarios en el sistema, crear o eliminar archivos, deshabilitar servicios y/o ejecutar código arbitrario de Java, y llevar a los atacantes a obtener el control total sobre el dispositivo BIG-IP.

La vulnerabilidad es tan peligrosa que recibió la puntuación de 10 sobre 10 en la escala de gravedad CVSSv3. Este puntaje indica que el error de seguridad es fácil de explotar,

automatizar, utilizarse en Internet y no requiere credenciales válidas o habilidades de codificación avanzadas para aprovecharlo.

Este es el segundo error con puntuación 10/10 en un dispositivo de red divulgado esta semana, después de revelarse un error crítico similar que afectaba a los dispositivos de firewall y VPN de Palo Alto Networks el lunes.

El Comando Cibernético de Estados Unidos emitió una advertencia al sector privado y gubernamental esta semana, para corregir el error de Palo Alto, ya que esperaban que los hackers extranjeros intentaran explotar la vulnerabilidad.

> *«La urgencia de reparar este error no puede ser subestimada. Un uso común de su tecnología es la descarga SSL. El compromiso total de un sistema podría, en teoría, permitir a alguien espiar el tráfico no cifrado dentro del dispositivo. Su sistema operativo está basado en Linux y, como la mayoría de los ADC (controladores de entrega de aplicaciones), se implementan en partes centrales de redes de alto acceso»,* dijo Nate Warfield, ex ingeniero de F5 Networks y actual investigador de seguridad de Microsoft.

Puedes ver más información sobre cómo protegerte contra la vulnerabilidad CVE-2020-5902 BIG-IP TMUI RCE en esta página oficial de F5.