Días después de que F5 lanzara parches para una vulnerabilidad crítica de ejecución remota de código que afectaba a su familia de productos BIG-IP, los investigadores de seguridad advierten que pudieron crear un exploit para la vulnerabilidad.

Rastreada como CVE-2022-1388, con puntuación CVSS de 9.8, la vulnerabilidad se relaciona con una omisión de autenticación REST de iControl que, de ser explotada exitosamente, podría conducir a la ejecución remota de código, lo que permitiría a un atacante obtener acceso inicial y tomar el control de un sistema afectado.

Esto podría ir desde la implementación de mineros de criptomonedas hasta la eliminación de shells web para ataques de seguimiento, como el robo de información y el ransomware.

> *«Hemos reproducido el nuevo CVE-2022-1388 en BIG-IP de F5. ¡Parche lo antes posible!»*, dijo Positive Technologies.

La vulnerabilidad de seguridad crítica afecta a las siguientes versiones de productos BIG-IP:

- 16.1.0 – 16.1.2
- 15.1.0 – 15.1.5
- 14.1.0 – 14.1.4
- 13.1.0 – 13.1.4
- 12.1.0 – 12.1.6
- 11.6.1 – 11.6.5

Las correcciones están disponibles en las versiones 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6 y 13.1.5. Las versiones de firmware 11.x y 12.x no recibirán actualizaciones de seguridad y los usuarios que confían en esas versiones deben considerar actualizar a una versión más nueva o aplicar las soluciones alternativas:

- Bloquee el acceso REST de iControl por medio de la propia dirección IP
- Bloquee el acceso REST de iControl a través de la interfaz de administración

- Modifique la configuración httpd de BIG-IP

El mes pasado, las autoridades de seguridad cibernética de Australia, Canadá, Nueva Zelanda, Reino Unido y Estados Unidos, advirtieron en conjunto que *«los actores de amenazas atacaron agresivamente las vulnerabilidades de software críticas recientemente reveladas contra amplios conjuntos de objetivos, incluidas las organizaciones del sector público y privado en todo el mundo».*

Debido a que la falla de F5 BIG-IP resultó trivial de explotar, se espera que los equipos de hackers maliciosos hagan lo mismo, por lo que es imperativo que las organizaciones afectadas actúen rápidamente para aplicar los parches.

Actualización: El investigador de seguridad cibernética, Kevin Beaumont, advirtió sobre los intentos de explotación activos detectados en la naturaleza, al mismo tiempo que alertó sobre la disponibilidad de una prueba de concepto (PoC) pública para la falla de ejecución del código.