BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-10
Fecha de publicación: 09/05/2024
Tema: Vulnerabilidades en productos de F5
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- F5 BIG-IP

Descripción:

Un grupo de investigadores han descubierto 5 vulnerabilidades en un componente que reside en la línea de productos BIG-IP de F5, que, al ser explotadas, otorga a los atacantes control administrativo total del dispositivo, que con esto, permite a los atacantes la creación de cuentas en cualquier activo de F5 administrado por el componente Next Central Manager, Las cuentas creadas no serán visibles desde el componente, así habilitando persistencia maliciosa dentro del entorno.

Cabe mencionar que, aún no se ha visto ninguna explotación activa de estas vulnerabilidades en el mundo, sin embargo, F5 sólo reconoció dos de ellas, con una puntuación de severidad de 7.5 y denominándose como:

- CVE-2024-21793: inyección Odata,, una vulnerabilidad que permite a los atacantes inyectar datos maliciosos en consultas Odata
- CVE-2024-26026; inyección SQL, que permite la ejecución de sentencias de SQL maliciosas.

Es importante también mencionar que, según el equipo que descubrió las vulnerabilidades, aún hay otras 3 vulnerabilidades que no ha reconocido F5, pero que ellos insisten que también son importantes, pues, entre ellas hay la posibilidad de que se explote un SSRF, otra es que se puede restablecer la contraseña de administrador sin autenticarse, y otra es una configuración en el algoritmo de hashing, pues se menciona que no es tan robusto, esto, dando posibilidad a ataques de fuerza bruta.

Impacto

Un actor malintencionado puede explotar las vulnerabilidades reconocidas por F5, permitiendo la creación de cuentas ocultas, así, obteniendo persistencia en los productos

de F5, así, teniendo la posibilidad del control total de toda la red de dispositivos administrados por Next Central Manager.

Solución

Las vulnerabilidades reconocidas por F5 fueron corregidas en la versión 20.2.0 de Next Central Manager, pero se desconoce si las vulnerabilidades que aún no reconocen fueron arregladas en este mismo parche.

Información adicional:

- https://www.bleepingcomputer.com/news/security/new-big-ip-next-central-manager-bugs-allow-device-takeover/
- https://arstechnica.com/security/2024/05/critical-vulnerabilities-in-big-ip-appliances-leave-big-networks-open-to-intrusion/
- https://arstechnica.com/security/2024/05/critical-vulnerabilities-in-big-ip-appliances-leave-big-networks-open-to-intrusion/

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com