BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2025-40
Fecha de publicación: 13/05/2025
Tema: PoC liberado para vulnerabildiad de BIG-IP de F5
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

La vulnerabilidad afecta a las siguientes ramas de F5 BIG-IP:

- 17.1.0 – 17.1.2
- 16.1.0 – 16.1.5
- 15.1.0 – 15.1.10

Descripción

Se ha descubierto una vulnerabilidad de alta gravedad, identificada como CVE-2025-31644 con CVSS de 8.7 (alta), en los sistemas BIG-IP de F5 que operan en modo Appliance. Esta vulnerabilidad podría permitir que usuarios administrativos autenticados ejecuten comandos bash arbitrarios y obtengan acceso root.

La vulnerabilidad CVE-2025-31644, con una calificación CVSS de 8.7 (alta), reside en el parámetro de archivo del comando "save", que se utiliza para almacenar archivos de configuración. Este parámetro se pasa de forma insegura a scripts de Perl o comandos del sistema subyacentes, lo que lo expone a la inyección de comandos mediante metacaracteres de shell, como las comillas invertidas (`). El parámetro 'file' del comando 'guardar' es vulnerable a un ataque de inyección de comandos.

El comando guardar es ampliamente accesible, solo los usuarios con privilegios de nivel de administrador pueden proporcionar rutas de archivos personalizadas, un detalle importante que limita la explotabilidad pero no disminuye el impacto potencial.

Recomendamos a los administradores de sistemas BIG-IP, tomar medidas de correción al respecto y aplicar las actualización, especialmente porque ya existen varios PoC sobre dicha vulnerabilidad publicados en el Internet, esto podría aumentar la posibilidad del desarrollo de exploit por parte de atacantes.

Solución

Las organizaciones que ejecutan BIG-IP en modo Appliance deben aplicar inmediatamente los parches del proveedor para las versiones afectadas. En el siguiente enlace podrá encontrar ayudas de como realizar la actualización de su rama (branch):
https://my.f5.com/manage/s/article/K84205182

Además, agregamos el enlace al boletin de seguridad publicado por el proveedor:
https://my.f5.com/manage/s/article/K000148591

Información adicional:

- https://my.f5.com/manage/s/article/K000148591
- https://securityonline.info/poc-released-cve-2025-31644-exploit-grants-root-access-on-f5-big-ip-via-appliance-mode-command-injection/
- https://www.wiz.io/vulnerability-database/cve/cve-2025-31644
- https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2025-31644

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.us

contact@cybolt.com

cybolt.com