Boletín de alerta

Boletín Nro.:
Fecha de publicación: 15/10/2025
Tema: Alerta 2025-85 Incidente de Seguridad F5
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- **Productos BIG-IP**

Descripción

En octubre de 2025, **F5 Networks** reveló un **incidente de seguridad significativo** que afectó a sus sistemas internos. La empresa confirmó que un **actor de amenazas altamente sofisticado, presuntamente respaldado por un estado-nación**, mantuvo **acceso persistente y prolongado** a ciertos entornos de F5 desde **agosto de 2025**, logrando **extraer archivos confidenciales** de sus sistemas de desarrollo y plataformas internas de gestión del conocimiento de ingeniería.

Según la investigación, los archivos exfiltrados incluían **fragmentos de código fuente de productos BIG-IP** y **detalles sobre vulnerabilidades aún no divulgadas** en desarrollo. Sin embargo, F5 indicó que **no se han identificado vulnerabilidades críticas o de ejecución remota de código que puedan ser explotadas activamente**, y **no existe evidencia de manipulación en su cadena de suministro de software** ni de alteraciones en sus procesos de desarrollo y lanzamiento.

Asimismo, la compañía confirmó que **no hubo acceso ni exfiltración de información sensible de clientes** proveniente de sus sistemas CRM, financieros o de soporte técnico. No obstante, un **pequeño porcentaje de archivos** obtenidos del entorno de gestión del conocimiento **contenían información de configuración o implementación de ciertos clientes**, por lo que F5 **contactará directamente a los afectados**.

Como parte de la respuesta al incidente, F5 implementó **medidas de contención exhaustivas**, incluyendo la **rotación de credenciales**, **refuerzo de controles de acceso**, **automatización de parches**, y **mejoras en la arquitectura de red**. Además, contrató a **CrowdStrike, Mandiant, NCC Group e IOActive** para apoyar las labores de investigación, validación y fortalecimiento de la seguridad.

La compañía también lanzó **actualizaciones de seguridad para sus principales productos —BIG-IP, F5OS, BIG-IP Next para Kubernetes, BIG-IQ y APM—**, disponibles en su **Notificación Trimestral de Seguridad (octubre 2025)**, e instó a todos los clientes a **actualizar sus sistemas de inmediato**.

Solución:

Entre las acciones preventivas y de fortalecimiento, F5 publicó:

- Actualizaciones del software BIG-IP . Ya están disponibles las actualizaciones para clientes BIG-IP, F5OS, BIG-IP Next para Kubernetes, BIG-IQ y APM. Si bien desconocemos vulnerabilidades críticas o de ejecución remota de código no reveladas, recomendamos encarecidamente actualizar su software BIG-IP lo antes posible. Puede encontrar más información sobre estas actualizaciones en la **Notificación Trimestral de Seguridad** .
- Inteligencia de amenazas . El soporte de F5 ofrece una guía de búsqueda de amenazas para fortalecer la detección y la monitorización en su entorno.
- Guía de refuerzo con verificación . Publicamos **las mejores prácticas** para reforzar sus sistemas F5 y hemos añadido comprobaciones de refuerzo automatizadas a la **herramienta de diagnóstico F5 iHealth** . Esta herramienta detectará las deficiencias, priorizará las acciones y proporcionará enlaces a guías de solución.
- Guía de integración y monitorización de SIEM . Recomendamos habilitar la transmisión de eventos de BIG-IP a su SIEM y proporcionamos instrucciones paso a paso para la configuración de syslog (**KB13080**) y la monitorización de intentos de inicio de sesión (**KB13426**). Esto mejorará su visibilidad y las alertas sobre inicios de sesión de administrador, autenticaciones fallidas y cambios de privilegios y configuración.

Información adicional:

- **https://my.f5.com/manage/s/article/K000154696**
- **https://my.f5.com/manage/s/article/K000156572**
- **https://www.sec.gov/Archives/edgar/data/1048695/000104869525000149/ffiv-20251015.htm**
- **https://thehackernews.com/2025/10/f5-breach-exposes-big-ip-source-code.html**