Alerta

Exfiltración de datos de F5 BIG-IP

COLCERT AL-20251017-080

TIC

TLP:CLEAR

En agosto de 2025, **F5** identificó un acceso persistente por parte de un actor de amenazas que exfiltró archivos de su entorno de desarrollo, incluyendo parte del código fuente de **BIG-IP**, su principal plataforma para la gestión del tráfico, balanceo de carga y seguridad de aplicaciones empresariales.

Aunque la compañía confirmó que no hubo alteraciones en su cadena de suministro ni explotación activa, **la exposición del código y de vulnerabilidades no reveladas incrementa la probabilidad alta de que surjan *exploits* dirigidos** en el corto a mediano plazo.

Este análisis busca anticipar los posibles impactos de dicho conocimiento comprometido sobre entornos que utilizan BIG-IP, orientando decisiones tempranas en actualización, monitoreo continuo y ciberdefensa preventiva, bajo un nivel de incertidumbre moderado debido a la naturaleza sigilosa del actor y la complejidad del entorno afectado.

NIVEL DE RIESGO

ALTO

¿Qué ha informado F5 sobre este caso?

- En agosto de 2025, F5 detectó que un **actor de amenazas de tipo estatal había mantenido acceso persistente a sistemas internos de F5**, específicamente al entorno de desarrollo de BIG-IP y a plataformas de gestión del conocimiento de ingeniería. Desde esos sistemas se descargaron archivos.
- Indicó que los archivos exfiltrados contenían parte del **código fuente de BIG-IP** y detalles de vulnerabilidades no reveladas en las que F5 estaba trabajando.
- Hasta el momento **no se tiene conocimiento de que las vulnerabilidades no reveladas hayan sido explotadas**, ni que el actor haya modificado su cadena de suministro, sus pipelines de compilación ni el código fuente en uso
- F5 declara que no hay evidencia de acceso o exfiltración en sus sistemas CRM, financieros, de soporte o iHealth, ni de que el actor haya modificado código fuente de NGINX o afectado sus servicios Silverline o Distributed Cloud.
- Medidas tomadas por F5:
  - Contrató a CrowdStrike, Mandiant y otros expertos para ayudar en la contención, remediación y análisis forense.
  - Rotó credenciales y reforzó controles de acceso en sus sistemas internos.
  - Mejoró la automatización de su inventario y parches, así como sus capacidades de monitoreo y detección de amenazas.
  - Fortaleció su arquitectura de red y controles en su entorno de desarrollo de productos.
  - Liberó actualizaciones de *software* para BIG-IP, F5OS, BIG-IP Next para Kubernetes, BIG-IQ y APM, e **instó a los clientes a aplicarlas cuanto antes**.
- Afirma que **algunos de los archivos exfiltrados contenían información de configuración o implementación para un porcentaje reducido de clientes**, y que se comunicará directamente con los clientes afectados según corresponda.

¿Cómo validar si la infraestructura F5 está potencialmente vulnerable?

1. **Verificar inventario y versiones**: confirmar todos los dispositivos BIG-IP / F5OS / BIG-IQ y sus builds, compararlos con las versiones parcheadas que publicó F5.
2. **Ejecución de iHealth**: iHealth es una plataforma oficial de diagnóstico y análisis de configuración creada por F5 Networks. Se debe correr iHealth y aplicar las recomendaciones indicadas por esta herramienta.
3. **Exposición de la interfaz de gestión**: verificar si la interfaz de administración del dispositivo **mgmt** está accesible desde Internet (es el vector de mayor riesgo según CISA), si es así se debe restringir inmediatamente a rangos de IP de específicas. Si la administración remota es necesaria, hacerla únicamente a través de un jump-host, un servidor intermedio seguro al que el administrador se conecta primero, y desde allí entra al F5.
4. **Detectar descargas inusuales**: buscar señales de transferencias a través de *scp*, *sftp*, *curl* a IP externas, generación frecuente de archivos de respaldo completo (UCS) con *timestamp* inusual, descargas de artefactos desde la ruta /var.

Impacto para Colombia y la región

- **Sectores afectados:** Gobierno, Financiero, Energía, TIC, Salud, Educación e Infraestructuras críticas.

- **Riesgo alto**: el actor de amenazas exfiltró parte del código fuente de **BIG-IP**, producto ampliamente utilizado en infraestructuras críticas de la región para balanceo de carga, seguridad de aplicaciones y gestión del tráfico. Este acceso al código y a vulnerabilidades no divulgadas otorga a los atacantes una ventaja técnica significativa para desarrollar *exploits* personalizados y evadir detecciones tradicionales.

Posibles consecuencias

- Compromisos de redes corporativas mediante la explotación de vulnerabilidades en BIG-IP.
- Exfiltración de información sensible de clientes y entidades gubernamentales.
- Movimiento lateral hacia sistemas críticos.
- Interrupciones operativas en servicios esenciales.
- Existe una alta probabilidad de que grupos cibercriminales adapten las técnicas utilizadas por el actor estatal para sus propias campañas, generando una cascada de ataques secundarios en Latinoamérica durante los próximos meses.

Implicaciones en seguridad digital

- Este incidente resalta la necesidad urgente de fortalecer la gestión de vulnerabilidades y actualizaciones en dispositivos de borde, así como de reducir la exposición de interfaces de administración en redes públicas. Para Colombia y la región, implica reforzar los mecanismos de coordinación entre Csirt sectoriales y nacionales, promover la adopción de políticas de *hardening* estandarizadas y fomentar una cultura de monitoreo continuo ante amenazas derivadas de código fuente comprometido.
- La situación subraya un punto crítico: la dependencia tecnológica de proveedores globales puede convertirse en un vector de riesgo sistémico si no se implementan controles locales robustos de seguridad y gobernanza digital.

Mitigaciones MITRE

MITIGACIÓN	CÓDIGO	RELEVANCIA
Network Segmentation (segmentación de red)	**M1030**	Reduce el riesgo de movimiento lateral y limita la exposición de interfaces de gestión aislando dispositivos críticos en una red de gestión separada o DMZ. En este caso ayuda a contener compromisos y evitar que un acceso a desarrollo o a un dispositivo expuesto permita comprometer más activos.
Limit Access to Resource Over Network (limitar acceso a recursos por red)	**M1035**	Restringe y controla quién puede conectarse a recursos administrativos (uso de jump hosts, VPN/ZTNA, gateways), obliga MFA y minimiza exposiciones públicas. Para BIG-IP esto reduce la probabilidad de accesos administrativos no autorizados que podrían facilitar exfiltración o abuso de funciones de configuración.
Encrypt Sensitive Information (cifrar información sensible)	**M1041**	Asegura que código fuente, backups y artefactos de configuración estén cifrados en reposo y tránsito; esto limita el valor usable de los datos exfiltrados (o dificulta su uso sin las claves) y reduce el impacto de fugas similares. Es relevante para proteger backups y repositorios relacionados con BIG-IP.
Gestión de cuentas privilegiadas (Privileged Account Management)	**M1026**	Controlar, limitar, auditar y rotar cuentas y credenciales administrativas en sistemas F5 y plataformas de desarrollo evita el abuso de credenciales comprometidas. Implementar PAM (vaulting, just-in-time, separación de funciones) y registrar sesiones administrativas reduce la ventana de oportunidad para que un actor persistente acceda y extraiga código.

Soluciones y mitigaciones disponibles

- Actualizar todos los dispositivos F5 BIG-IP, F5OS y BIG-IQ a las versiones más recientes publicadas en la notificación de seguridad trimestral de octubre de 2025. Estas versiones incorporan correcciones y mejoras de seguridad que reducen el riesgo de explotación de vulnerabilidades no reveladas o derivadas del código fuente filtrado.

- Restringir el acceso público a las interfaces de administración de BIG-IP y demás productos F5, garantizando que solo sean accesibles desde redes internas o mediante conexiones seguras y autenticadas (por ejemplo, VPN con MFA). Las interfaces de gestión expuestas a Internet representan un vector de ataque crítico que debe ser eliminado de inmediato.

- Desconectar los dispositivos F5 que hayan alcanzado su fin de soporte (End of Support), dado que no recibirán actualizaciones ni parches de seguridad. Estos activos deben ser reemplazados o aislados completamente del entorno productivo para prevenir su uso como puntos de entrada para actores hostiles.

- Implementar controles de monitoreo y alertamiento en el SIEM institucional, configurando la transmisión de logs desde BIG-IP y F5OS para detectar intentos de acceso no autorizado, autenticaciones fallidas, cambios de configuración y actividades anómalas en las cuentas administrativas. La visibilidad temprana permitirá identificar posibles intentos de explotación antes de que se materialicen.

- Fortalecer la gestión de credenciales y accesos privilegiados en los entornos F5 mediante la rotación inmediata de contraseñas administrativas, la aplicación de autenticación multifactor y la reducción del número de cuentas con privilegios elevados. Esto limita el impacto en caso de compromiso de credenciales derivado del incidente.

Fuentes

F5, 15 oct 2025, K000156572 (fuente oficial de F5), portal de soporte de F5.
https://my.f5.com/manage/s/article/K000156572
F5, 15 oct 2025, K000154696: Incidente de seguridad de F5 (fuente oficial de F5), portal de soporte de F5. ://my.f5.com/manage/s/article/K000154696
CISA, 15 oct 2025, 15 oct 2025, Emergency Directive ED 26-01: Mitigate Vulnerabilities in F5 Devices (directiva gubernamental), sitio oficial de CISA.
https://www.cisa.gov/news-events/directives/ed-26-01-mitigate-vulnerabilities-f5-devices
BleepingComputer, 15 oct 2025, , Hackers breach F5 to steal undisclosed BIG-IP flaws, source code (medio de noticias), sitio informativo de ciberseguridad.
https://www.bleepingcomputer.com/news/security/hackers-breach-f5-to-steal-undisclosed-big-ip-flaws-source-code/