I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Ejecución código remoto en F5 BIG-IP
Nivel de riesgo: Crítico

II. ALERTA

EL 27 de octubre de 2023, F5 reveló una vulnerabilidad de gravedad crítica que afecta a sus sistemas BIG-IP.

Figura No. 1.- Ilustración asociada a F5
Fuente: https://latesthackingnews.com/2023/10/30/critical-f5-big-ip-flaw-allows-remote-code-execution-attacks/

III. INTRODUCCIÓN

BIG-IP es un conjunto de soluciones de hardware y software dedicado que facilita el control de acceso, la disponibilidad y la seguridad de las aplicaciones. Dadas sus funcionalidades, BIG-IP cuenta con una gran cantidad de clientes, lo que también indica el alcance de los usuarios vulnerables en caso de cualquier exploit de BIG-IP.

F5 informó que existe una falla de seguridad crítica en la utilidad de configuración F5 BIG-IP que permite a un atacante ejecutar comandos arbitrarios. En el peor de los casos, un atacante que tenga acceso previo a la red objetivo puede explotar fácilmente la vulnerabilidad.

El 25 de octubre de 2023, fue publicado el CVE-2023-46747, relacionado con una vulnerabilidad de autenticación de la utilidad de configuración, lo que permite a un atacante con acceso de red al sistema BIG-IP a través del puerto de administración y/o direcciones IP propias, ejecutar comandos arbitrarios del sistema. La vulnerabilidad

reportada con el CVE-2023-46747, recibió una calificación de gravedad crítica con una puntuación CVSS versión 3.x de 9,8.

F5 ha lanzado nuevas versiones que incluyen parches de seguridad, e insta a los usuarios a actualizar sus versiones.

IV. VECTOR DE ATAQUE:

La vulnerabilidad permite que un atacante no autenticado con acceso de red al sistema BIG-IP a través del puerto de administración logre la ejecución del código.

Versiones afectadas (Utilidad de configuración)
• 17.1.0 - 17.1.1 (Corregido en 17.1.0.3 + Hotfix-BIGIP-17.1.0.3.0.75.4-ENG) • 16.1.0 - 16.1.4 (Corregido en 16.1.4.1 + Hotfix-BIGIP-16.1.4.1.0.50.5-ENG) • 15.1.0 - 15.1.10 (Corregido en 15.1.10.2 + Hotfix-BIGIP-15.1.10.2.0.44.2-ENG) • 14.1.0 - 14.1.5 (Corregido en 14.1.5.6 + Hotfix-BIGIP-14.1.5.6.0.10.6-ENG) • 13.1.0 - 13.1.5 (Corregido en 13.1.5.1 + Hotfix-BIGIP-13.1.5.1.0.20.2-ENG)

Tabla No. 1.- Versiones afectadas de F5 BIG-IP
Fuente: https://thehackernews.com/2023/11/alert-f5-warns-of-active-attacks.html

V. IMPACTO:

La vulnerabilidad permite que un atacante no autenticado con acceso de red al sistema BIG-IP a través del puerto de administración y/o direcciones IP propias ejecute comandos arbitrarios del sistema. “No hay exposición al plano de datos; Este es un problema únicamente del plano de control” (Myf5, s.f.).

VI. INDICADORES DE COMPROMISO

No aplica

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo:

- Aplicar las actualizaciones provistas F5 BIG-IP.
- Eliminar archivos y cuentas de usuario no autorizados y restablecer las credenciales de la cuenta de servicio.
- Actualizar las reglas del firewall, para permitir únicamente conexiones a la infraestructura desde direcciones IP conocidas, configurar el firewall del sistema para bloquear el tráfico malicioso.

- Actualizar las políticas de acceso remoto para permitir solo conexiones entrantes desde direcciones IP conocidas y confiables.
- Consultar los avisos para el CVE-2023-46747 para aplicar los parches correspondientes.
- Mantener actualizado el software del sistema operativo y las aplicaciones, pero actuar con precaución al aplicar los parches de seguridad, y utilizar los más recientes siempre que sea posible.
- Monitorear de manera proactiva las relaciones de ejecución de procesos anormales y tomar medidas preventivas para evitar actividades como la exfiltración de información.

Con estas recomendaciones de seguridad, se puede minimizar las posibilidades de ser una víctima, las recomendaciones no garantizan la seguridad, pero ayudan a reducir el riesgo.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- *CVE - CVE-2023-46747*. (s. f.). https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-46747
- Hashim, A., & Hashim, A. (2023, 30 octubre). *Critical F5 BIG-IP flaw allows remote code execution attacks*. Latest Hacking News | Cyber Security News, Hacking Tools and Penetration Testing Courses. https://latesthackingnews.com/2023/10/30/critical-f5-big-ip-flaw-allows-remote-code-execution-attacks/
- *MyF5*. (s. f.). https://my.f5.com/manage/s/article/K000137353
- *NVD - CVE-2023-46747*. (s. f.). https://nvd.nist.gov/vuln/detail/CVE-2023-46747
- The Hacker News. (s. f.-a). *Alert: F5 warns of active attacks exploiting BIG-IP vulnerability*. https://thehackernews.com/2023/11/alert-f5-warns-of-active-attacks.html
- The Hacker News. (s. f.-b). *F5 Issues Warning: BIG-IP vulnerability allows remote code execution*. https://thehackernews.com/2023/10/f5-issues-warning-big-ip-vulnerability.html