El proveedor de dispositivos de red y seguridad empresarial F5 publicó parches para más de 24 vulnerabilidades de seguridad que afectan a múltiples versiones de dispositivos BIG-IP y BIG-IQ, que podrían permitir a un atacante realizar una amplia gama de acciones maliciosas, incluyendo el acceso a archivos arbitrarios, escalando privilegios y ejecutando código JavaScript.

De los 29 errores solucionados, 13 son vulnerabilidades de alta gravedad, 15 de media gravedad y uno de baja gravedad.

La principal vulnerabilidad, CVE-2021-23031, con puntuación CVSS de 8.8, es una falla que afecta a BIG-IP Advanced Web Application Firewall y BIG-IP Application Security Manager, que permite a un usuario autenticado realizar una escalada de privilegios.

> *«Cuando se explota esta vulnerabilidad, un atacante autenticado con acceso a la utilidad de configuración puede ejecutar comandos arbitrarios del sistema, crear o eliminar archivos y/o deshabilitar servicios. Esta vulnerabilidad puede resultar en un compromiso total del sistema»,* dijo F5 en su aviso.

Cabe mencionar que para los clientes que ejecutan en modo de dispositivo, que aplica restricciones técnicas adicionales en sectores sensibles, la misma vulnerabilidad cuenta con una calificación crítica de 9.9.

> *«Como este ataque lo llevan a cabo usuarios legítimos y autenticados, no hay mitigación viable que también permita a los usuarios acceder a la utilidad de configuración. La única mitigación es eliminar el acceso a los usuarios que no son completamente confiables»,* dijo la compañía.

Otras vulnerabilidades importantes resueltas por F5 son:

- CVE-2021-23025 (puntuación CVSS de 7.2): Vulnerabilidad de ejecución de comandos remotos autenticados en la utilidad de configuración BIG-IP.
- CVE-2021-23026 (puntuación CVSS de 7.5): Vulnerabilidad de falsificación de solicitudes entre sitios (CSRF) en iControl SOAP.
- CVE-2021-23027 y CVE-2021-23037 (puntuación CVSS de 7.5): Vulnerabilidades de secuencias de comandos de sitios cruzados (XSS) basadas en DOM de TMUI y reflejadas.
- CVE-2021-23028 (puntuación CVSS de 7.5): Vulnerabilidad de WAF y ASM avanzada de BIG-IP.
- CVE-2021-23029 (puntuación CVSS de 7.5): Vulnerabilidad de BIG-IP Advanced WAF y ASM TMUI.
- CVE-2021-23030 y CVE-2021-23033 (puntuación CVSS de 7.5): Vulnerabilidades de BIG-IP Advanced WAF y ASM Websocket.
- CVE-2021-23034, CVE-2021-23035 y CVE-2021-23026 (puntuación CVSS de 7.5): Vulnerabilidades del microkernel de gestión del tráfico.

Además, F5 también corrigió una serie de vulnerabilidades que van desde la vulnerabilidad de recorrido de directorio y la inyección de SQL hasta la vulnerabilidad de redireccionamiento abierto y la falsificación de solicitudes entre sitios, así como una falla en la base de datos MySQL que hace que la base de datos consuma más espacio de almacenamiento de lo esperado cuando las funciones de protección de fuerza bruta del cortafuegos están habilitadas.

Debido a que los dispositivos F5 por lo general se convierten en objetivos jugosos para los intentos de explotación activos por parte de los actores de amenazas, se recomienda encarecidamente que los usuarios y administradores instalen software actualizado o apliquen las mitigaciones necesarias lo más rápido posible.