Un fallo crítico que afecta a determinados routers Four-Faith ha sido detectado en ataques activos, según un informe reciente de VulnCheck.

La vulnerabilidad, registrada como CVE-2024-12856 (con una puntuación CVSS de 7.2), se clasifica como un fallo de inyección de comandos del sistema operativo (OS) que compromete los modelos de routers F3x24 y F3x36.

Aunque la gravedad del problema es moderada, esto se debe a que el ataque solo puede llevarse a cabo si el atacante logra autenticarse. Sin embargo, si las credenciales predeterminadas del dispositivo no han sido modificadas, el fallo permite la ejecución de comandos en el sistema operativo sin necesidad de autenticación.

Según VulnCheck, los atacantes han aprovechado las credenciales por defecto de los routers para explotar la vulnerabilidad CVE-2024-12856, estableciendo un shell inverso que les otorga acceso remoto persistente.

El ataque fue rastreado hasta la dirección IP 178.215.238[.]91, que anteriormente se asoció con intentos de explotar CVE-2019-12168, otra vulnerabilidad de ejecución remota de código en dispositivos Four-Faith. La firma de ciberseguridad GreyNoise confirmó que los intentos de explotar CVE-2019-12168 continuaron hasta el 19 de diciembre de 2024.

> *«El ataque puede ejecutarse, al menos, en los modelos F3x24 y F3x36 de Four-Faith a través del protocolo HTTP, utilizando el endpoint /apply.cgi. La inyección de comandos del sistema operativo se produce en el parámetro adj_time_year al modificar la hora del sistema del dispositivo mediante submit_type=adjust_sys_time»*, explicó Jacob Baines en su análisis.

Censys reportó que existen más de 15,000 dispositivos accesibles públicamente en internet. Además, algunos indicios sugieren que los ataques que explotan esta vulnerabilidad han estado ocurriendo desde principios de noviembre de 2024.

Por el momento, no hay información sobre la disponibilidad de actualizaciones o parches para corregir este problema. VulnCheck indicó que notificó la vulnerabilidad de forma responsable a la empresa Four-Faith el 20 de diciembre de 2024.