Los hackers están explotando activamente una vulnerabilidad sin parches, de cinco años de antigüedad, que afecta a los dispositivos de grabación de video digital (DVR) TBK, según un aviso emitido por Fortinet FortiGuard Labs.

La vulnerabilidad en cuestión es CVE-2018-9995 (puntaje CVSS: 9.8), una vulnerabilidad crítica de omisión de autenticación que poría ser explotada por hackers remotos para obtener permisos elevados.

> *«La vulnerabilidad de 5 años (CVE-2018-9995) se debe un error al manejar una cookie HTTP creada con fines malintencionados. Un atacante remoto puede aprovechar esta vulnerabilidad para eludir la autenticación y obtener privilegios administrativos eventualmente conduce al acceso a las transmisiones de video de la cámara»,* dijo Fortinet en una alerta de brote el 1 de mayo de 2023.

La compañía de seguridad de red dijo que observó más de 50,000 intentos de explotar los dispositivos DVR TBK usando la vulnerabilidad en el mes de abril de 2023. A pesar de la disponibilidad de un exploit de prueba de concepto (PoC), no existen soluciones que aborden la vulnerabilidad.

La vulnerabilidad afecta las líneas de productos TBK DVR4104 y DVR4216, que también se renombran y venden con los nombres CeNova, DVR Login, HVR Login, MDVR Login, Night OWL, Novo, QSee, Pulnix, securus y XVR 5 en 1.

Además, Fortinet advirtió sobre un aumento en la explotación de CVE-2016-20016 (puntaje CVSS: 9.8), otra vulnerabilidad crítica que afecta a los modelos de DVR CCTV de MVPower, incluidos TV-7104HE 1.8.4 115215B9 y TV7108HE.

La vulnerabilidad podría permitir que un hacker remoto no autenticado ejecute comandos arbitrarios del sistema operativo como root debido a la presencia de un shell web al que se puede acceder por medio de un URI/shell.

> *«Con decenas de miles de DVR TBK disponibles bajo distintas marcas, código PoC disponible públicamente y fácil de explotar, esta vulnerabilidad es un objetivo fácil para los atacantes. El aumento reciente en las detecciones de IPs muestra que los dispositivos de cámara de red siguen siendo un objetivo popular para los atacantes»,* dijo Fortinet.