Vladislav Yarmak, investigador de seguridad ruso, publicó hoy los detalles sobre un mecanismo de puerta trasera que descubrió en chips HiSilicon, utilizados por millones de dispositivos inteligentes en todo el mundo, como cámaras de seguridad, DVR, NVR, entre otros.

Actualmente no existe una solución de firmware ya que Yarmak no informó el problema a HiSilcon, citando una falta de confianza en el proveedor para solucionar el problema de la forma más adecuada.

Yarmak publicó un resumen técnico en Habr, donde asegura que el mecanismo de «*backdoor*» es en realidad una combinación de cuatro errores (puertas traseras) de seguridad más antiguos que se descubrieron inicialmente y se hicieron públicos en marzo de 2013, marzo de 2017, julio de 2017 y septiembre de 2017.

> *«Aparentemente, durante todos esos años HiSilicon no estuvo dispuesto o fue incapaz de proporcionar soluciones de seguridad adecuadas para la misma puerta trasera que, por cierto, se implementó intencionalmente»*, dijo Yarmak.

El investigador dice que la puerta trasera se puede explotar enviando una serie de comandos por medio del puerto TCP 9530 a dispositivos que utilizan chips de la compañía. Los comandos habilitan el servicio Telnet en un dispositivo vulnerable.

Según Yarmak, una vez que el servicio Telnet está en funcionamiento, el atacante puede iniciar sesión con una de las seis credenciales de Telnet que se enumeran a continuación, y obtener acceso a una cuenta raíz que les otorga control total sobre un dispositivo vulnerable.

Estos inicios de sesión de Telnet se han encontrado en años anteriores como codificados en el firmware del chip HiSilicon, pero a pesar de los informes públicos, Yarmak asegura que el proveedor decidió dejarlos intactos y desactivar el daemon Telnet.

Debido a que el investigador no tenía la intención de informar sobre la vulnerabilidad a HiSilicon, los parches de firmware no están disponibles. En lugar de eso, el investigador creó un código de prueba de concepto (PoC) que puede utilizarse para probar si un dispositivo inteligente se está ejecutando sobre el sistema en chip HiSilicon (SoC) y si ese SoC es vulnerable a ataques que puedan habilitar su servicio Telnet.

Si se descubre que un dispositivo es vulnerable, en su informe de Habr, el investigador insiste en que los propietarios de dispositivos deben deshacerse y reemplazar el equipo.

> *«Teniendo en cuenta las correcciones falsas anteriores para esa vulnerabilidad, no es práctico esperar correcciones de seguridad para el firmware del proveedor. Los propietarios de dichos dispositivos deberían considerar cambiar a alternativas»*, dijo Yarmak.

En el caso de que los propietarios de dispositivos no puedan pagar el precio del nuevo equipo, Yarmak recomienda que los usuarios *«deberían restringir por completo el acceso de red a estos dispositivos a usuarios confiables»,* especialmente en los puertos de dispositivo 23/tcp, 95307tcp, 9527/tcp, los puertos que pueden explotarse en ataques.

El código de prueba de concepto está disponible en GitHub y las instrucciones de compilación y uso están disponibles en el artículo de Habr.

Sobre el impacto, Yarmak dijo que los chips HiSilicon vulnerables probablemente se envían con dispositivos de innumerables proveedores de marca blanca, bajo numerosas marcas y etiquetas. En este punto, citó el trabajo de otro investigador que en septiembre de 2017 rastreó un mecanismo de puerta trasera similar en el firmware HiSilicon que estaba siendo utilizado por los DVR vendidos por decenas de proveedores.