Los investigadores de seguridad cibernética detallaron hasta cinco vulnerabilidades de seguridad graves en la implementación del protocolo TLS en varios modelos de switches de red de Aruba y Avaya, que podrían utilizarse para obtener acceso remoto a redes empresariales y robar información valiosa.

Los hallazgos siguen a la divulgación de marzo de TLStorm, un conjunto de tres vulnerabilidades críticas en los dispositivos Smart-US de APC, que podrían permitir que un atacante tome el control y dañe de forma física los dispositivos.

La compañía de seguridad de IoT, Armis, que descubrió las vulnerabilidades, dijo que las fallas de diseño se remontan a una fuente común: un mal uso de NanoSSL, una suite de desarrollo SSL basada en estándares de Mocana, una subsidiaria de DigiCert.

El nuevo conjunto de vulnerabilidades, denominado TLStorm 2.0, hace que los switches de red de Aruba y Avaya sean vulnerables a vulnerabilidades de ejecución remota de código, lo que permite que un adversario controle los dispositivos, se mueva lateralmente a través de la red y exfiltre datos confidenciales.

Los dispositivos afectados incluyen Avaya ERS3500 Series, ERS3600 Series, ERS4900 Series y ERS5900 Series, así como Aruba 5400R Series, 3810 Series, 2920 Series, 2930F Series, 2930M Series, 2530 Series y 2540 Series.

Armis atribuyó las fallas a un *«caso límite»*, la falta de cumplimiento de las pautas relacionadas con la biblioteca NanoSSL que podría resultar en la ejecución remota de código. La lista de errores de ejecución remota de código es la siguiente:

- CVE-2022-23676 (puntuación CVSS: 9.1): Dos vulnerabilidades de corrupción de memoria en la implementación del cliente RADIUS de los switches Aruba.
- CVE-2022-23677 (puntuación CVSS: 9.0): Uso indebido de NanoSSL en múltiples interfaces en switches Aruba.
- CVE-2022-29860 (puntuación CVSS: 9.8): Vulnerabilidad de desbordamiento del

montón de reensamblaje de TLS en los switches Avaya.

- CVE-2022-29861 (puntuación CVSS: 9.8): Vulnerabilidad de desbordamiento de pila de análisis de encabezado HTTP en switches Avaya.
- Vulnerabilidad de desbordamiento de montón en el manejo de solicitudes HTTP POST en una línea de productos Avaya descontinuada (sin SVE).

> *«Estos resultados de la investigación son significativos, ya que destacan que la infraestructura de la red en sí está en riesgo y es explotable por los atacantes, lo que significa que la segmentación de la red por sí sola ya no es suficiente como medida de seguridad»,* dijo Barak Hadad, jefe de investigación en ingeniería de Armis.

Se recomienda a las organizaciones que utilizan dispositivos Avaya y Aruba afectados, que apliquen los parches para mitigar cualquier posible intento de explotación.