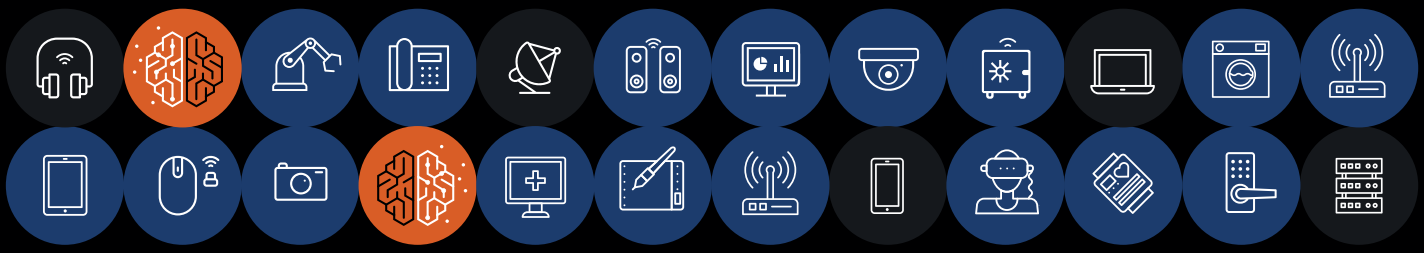
FORESCOUT
Active Defense for the Enterprise of Things™

AMNESIA:33

Resumen ejecutivo del informe de investigación



- Forescout Research Labs ha lanzado Project Memoria, **una iniciativa** que pretende proporcionar a la comunidad el **mayor estudio sobre seguridad de las pilas TCP/IP**. El objetivo de Project Memoria es ampliar el conocimiento de los errores comunes que se hallan detrás de las vulnerabilidades de las pilas TCP/IP, identificando las amenazas que representan para la empresa ampliada y la manera de mitigarlas.
- **AMNESIA:33** es el primer estudio de Project Memoria que hemos publicado. En este estudio, describimos los resultados del análisis de seguridad de siete **pilas TCP/IP de código abierto** e informamos de un paquete de **33 nuevas vulnerabilidades** localizadas en cuatro de las siete pilas analizadas que utilizan destacados proveedores de dispositivos IoT, OT e IT.
- **Cuatro de las vulnerabilidades de AMNESIA:33 son críticas**, con potencial para la ejecución de código remoto en determinados dispositivos. Si aprovecha estas vulnerabilidades, el atacante puede hacerse con el control de un dispositivo y utilizarlo como punto de entrada a una red para acceder a los dispositivos conectados a Internet, como punto de inicio de desplazamiento lateral, como punto de persistencia en la red de destino o como el objetivo último del ataque. En las grandes empresas, esto implica un riesgo mayor de compromiso de la red o de interrupción de la actividad del negocio. Para los usuarios particulares, significa que sus dispositivos IoT pueden utilizarse como parte de campañas de ataque mayores, como las de redes de bots, sin que ellos sean conscientes.

Más de 150

PROVEEDORES AFECTADOS

forescout.com/amnesia33/ info-espana@forescout.com Tel. (internacional) +1-408-213-3191

- AMNESIA:33 afecta a **varias pilas TCP/IP de código abierto** que **no son propiedad de una sola empresa**. Por este motivo, una sola vulnerabilidad tiende a **propagarse de forma rápida y desapercibida** por varias bases de código, equipos de desarrollo, empresas y productos, lo que dificulta en gran medida la administración de parches.
- Calculamos que más de 150 proveedores y millones de dispositivos son vulnerables a AMNESIA:33. Sin embargo, **es difícil evaluar el impacto total** de AMNESIA:33, ya que las pilas vulnerables están muy distribuidas (en distintos dispositivos IoT, OT e IT de sectores diferentes), son muy modulares (con componentes, funciones y configuraciones en varias combinaciones y bases de código con frecuentes bifurcaciones) y están incorporadas en subsistemas no documentados y muy incrustados. Por los mismos motivos, suele ser difícil erradicar estas vulnerabilidades.
- Las pilas TCP/IP afectadas por AMNESIA:33 se encuentran en sistemas operativos para dispositivos incrustados, sistemas en chip, equipamiento de red, dispositivos OT e innumerables dispositivos IoT para empresas y particulares.
- Las pilas TCP/IP son componentes esenciales de todos los dispositivos conectados por IP, incluidos los IoT y OT, ya que permiten la comunicación de red básica. Un fallo en la seguridad de una pila TCP/IP puede ser extremadamente peligroso, debido a que el código de estos componentes se puede utilizar **para procesar *todos* los paquetes de red entrantes que lleguen a un dispositivo**. Esto significa que algunas vulnerabilidades de una pila TCP/IP permiten atacar un dispositivo incluso con que solo se conecte a una red, sin necesidad de que ejecute una aplicación específica.
- Muchas de las vulnerabilidades comunicadas en **AMNESIA:33** se producen como resultado de malas prácticas de desarrollo de software, como la inexistencia de validación de entradas básica. Están relacionadas principalmente con la **corrupción de memoria** y pueden provocar **denegaciones de servicio, filtraciones de información** o **ejecución de código remoto**.
- Debido a la complejidad de la identificación y aplicación de parches en los dispositivos vulnerables, la gestión de vulnerabilidades para pilas TCP/IP está siendo un verdadero reto para la comunidad de seguridad. Recomendamos que **se adopten soluciones que ofrezcan visibilidad granular de los dispositivos**, permitan la supervisión de las comunicaciones de red y aíslen los dispositivos o segmentos de red vulnerables para gestionar el riesgo que representan estas vulnerabilidades.

No se conforme con verlo. Protéjalo.

Póngase en contacto con nosotros hoy mismo para proteger su Empresa de las cosas.

Descargue el informe completo (en inglés): Vea los detalles de nuestra investigación y descubra qué técnicas de mitigación puede aplicar.

Descargue el libro blanco (en inglés): Descubra cómo le ayuda Forescout a defenderse de forma activa contra AMNESIA:33, junto a seis mejores prácticas para proteger su organización.

Vea el seminario web (en inglés): Escuche a nuestros expertos que describen lo más interesante de la investigación.

forescout.com/amnesia33/ info-espana@forescout.com Tel. (internacional) +1-408-213-3191

FORESCOUT
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
San José, CA 95134 EE. UU.

C. e.: info-espana@forescout.com
Tel. (internacional) +1-408-213-3191
Soporte técnico +1-708-237-6591

Más información en Forescouttechnologies.es