Se han identificado casi dos docenas de fallos de seguridad en los dispositivos de puntos de acceso inalámbricos industriales Advantech EKI, algunos de los cuales podrían ser utilizados para evitar la autenticación y ejecutar código con permisos elevados.

> *«Estas vulnerabilidades presentan riesgos considerables, ya que permiten la ejecución remota de código sin autenticación con privilegios de administrador, lo que compromete por completo la confidencialidad, integridad y disponibilidad de los dispositivos afectados»,* explicó Nozomi Networks, una compañía de ciberseguridad, en un análisis publicado el miércoles.

Después de una divulgación responsable, los problemas fueron corregidos en las siguientes versiones de firmware:

- 1.6.5 (para EKI-6333AC-2G y EKI-6333AC-2GD)
- 1.2.2 (para EKI-6333AC-1GPO)

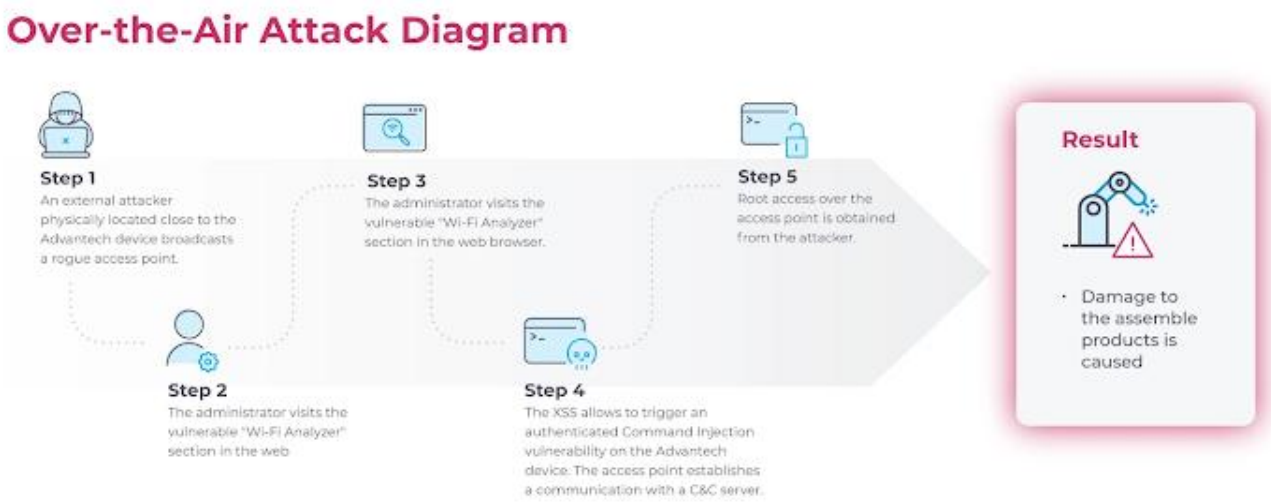
Vulnerabilidades críticas

De las 20 vulnerabilidades detectadas, seis se consideran críticas. Estas podrían permitir a un atacante obtener acceso persistente a recursos internos mediante la instalación de una puerta trasera, causar una denegación de servicio (DoS) o incluso reutilizar los puntos de acceso comprometidos como estaciones Linux para realizar movimientos laterales e infiltrarse más en la red.

Cinco de estas fallas (CVE-2024-50370 a CVE-2024-50374, con puntuaciones CVSS de 9.8) están relacionadas con la manipulación inadecuada de elementos especiales en comandos del sistema operativo. La sexta, CVE-2024-50375 (también con una puntuación CVSS de 9.8), se refiere a la ausencia de autenticación en una función clave.

Otro fallo relevante, CVE-2024-50376 (CVSS: 7.3), es una vulnerabilidad de cross-site scripting (XSS) que podría combinarse con CVE-2024-50359 (CVSS: 7.2), una inyección de

comandos en el sistema operativo que normalmente requiere autenticación, para permitir la ejecución remota de código sin cables.



Condiciones para el ataque

Para explotar estas vulnerabilidades, un atacante externo debe encontrarse cerca físicamente del punto de acceso Advantech y emitir una señal de punto de acceso malicioso. El ataque se desencadena cuando un administrador accede a la sección «Wi-Fi Analyzer» en la aplicación web. La página procesa automáticamente información de las tramas beacon enviadas por el atacante sin realizar comprobaciones de seguridad.

> *«Por ejemplo, el atacante podría transmitir un nombre de red Wi-Fi (SSID) malicioso que incluya un fragmento de código JavaScript. Esto le permitiría explotar CVE-2024-50376, desencadenando un ataque XSS dentro de la aplicación web»,* señaló Nozomi Networks.

Consecuencias del ataque

El código JavaScript malicioso podría ejecutarse en el navegador del administrador afectado. Si se combina con CVE-2024-50359, permitiría inyectar comandos en el sistema operativo con privilegios de administrador, por ejemplo, estableciendo una conexión remota persistente mediante un *shell* inverso.

> *«Con esto, los atacantes podrían controlar el dispositivo comprometido, ejecutar comandos y moverse dentro de la red para robar información o desplegar scripts maliciosos adicionales»*, concluyó la empresa.