Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE)

AuthUsb SafeDoor

Control de versiones

Versión	Comentario	Fecha
1	Inicial	20 nov 2018
2	Revisión amenazas	6 dic 2018
3	Revisión seguridad	25 ene 2019
4	Revisión seguridad	27 mar 2019
5	Revisión seguridad	29 Abril 2019
6	Revisión seguridad	11 May 2022
7	Número de versión	08 Nov 2022
8	Número de versión	21 Feb 2023
9	Número de versión	24 Abril 2023

1. Introducción

Este documento constituye la declaración de seguridad del producto **authUsb Safedoor**, dispositivo hardware para la protección contra amenazas derivadas del uso de memorias USB

1.1. Información del patrocinador, TOE y evaluación

Datos del patrocinador	
Datos del desarrollador	authUsb
Datos de contacto del desarrollador	Jorge Vega Lamas jvega@authusb.com 605869373
Nombre del TOE	authUsb safeDoor
Versión del TOE	2.0.0.11
Tipo de evaluación	LINCE
Manual de uso	Manual safeDoor v1.4.pdf
Taxonomía del producto CCN-STIC-140	Otras herramientas

1.2. Metodología y criterios de evaluación

CCN-LINCE-001	CCN-LINCE-001 - Definición de la Certificación Nacional Esencial de Seguridad
CCN-LINCE-002	CCN-LINCE-002 - Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad Versión 0.1, Junio de 2018

2. Descripción del TOE

El TOE se compone de un único elemento físico contenido en una carcasa de aluminio con conectores para alimentación, un puerto ethernet, dos puertos USB y tres LEDs de estado.

Aún cuando en su operativa normal interactúa con otros elementos (navegador web del cliente, memorias USB, red local) éstos no forman parte del TOE

2.1. Descripción funcional del TOE

authUsb safeDoor es un dispositivo hardware que actúa como barrera entre las memorias USB y los equipos de una organización, identificando amenazas a tres niveles:

- Eléctrico:
  Monitoriza continuamente el comportamiento de la memoria USB a nivel eléctrico, identificando y deteniendo ataques destructivos de sobretensión tipo UsbKiller (https://usbkill.com/)
- Hardware:
  Monitoriza continuamente el comportamiento de la memoria USB a nivel hardware, detectando y desactivando ataques de la familia BadUsb, ataques HID (rubber ducky y similares), falsas tarjetas de red, interfaces compuestas, etc
- Software
  Dispone de un antivirus integrado (compatible con varios fabricantes) con el que realiza un análisis previo a la descarga de cualquier contenido.

Safedoor ofrece dos conectores hembra USB tipo A para la introducción de memorias USB a analizar y un puerto ethernet para su conexión a la red o punto a punto directamente a un ordenador. A través de esta conexión de red ofrece una interfaz web para la interacción con el usuario

2.2. Guía de instalación y uso

Manual de usuario	Manual Safedoor v1.4.pdf
Guia de instalación rápida	Guia de instalación SafeDoor v2.pdf

2.3. Modo de uso

Cualquier memoria USB externa debe ser conectada únicamente al dispositivo SafeDoor, nunca deben tener contacto directo con ningún equipo de la organización.

- Paso 1: El usuario conecta una memoria USB a Safedoor en uno de sus puertos USB. El LED del puerto se encenderá en color naranja durante unos segundos mientras se lleva a cabo el análisis eléctrico y hardware.
    - En caso de detectar una amenaza el LED cambiará a rojo y se desactivará la memoria USB
    - Si el análisis es satisfactorio el LED cambiará a Verde
- Paso 2: El usuario, desde un ordenador conectado a la misma red (o directamente al dispositivo a través del puerto ethernet), abrirá en un navegador web la url del SafeDoor (por ejemplo, https://authusb/) accediendo a la aplicación alojada en el servidor web embebido en el dispositivo. En caso de detección de amenaza se mostrará un mensaje descriptivo y se bloqueará el acceso a la memoria USB

- Paso 3: Superado el análisis eléctrico y hardware, el usuario podrá navegar la estructura de carpetas y archivos contenidos en la memoria a través de la aplicación web. Una vez seleccionados los archivos o carpetas deseados, pulsará el botón Analizar. En este punto el antivirus embebido del SafeDoor realizará un análisis en busca de malware.
    - En caso de detección de malware lo notificará al usuario y bloqueará el acceso a los archivos. El LED del puerto USB cambiará a Rojo
    - Si el análisis es satisfactorio comenzará la descarga de los ficheros solicitados, agrupados en un único fichero zip.

3. Entorno de ejecución

3.1. Descripción del entorno de ejecución

Material necesario:

- Dispositivo SafeDoor, alimentación y cable ethernet
- Ordenador cliente, Windows, linux o Mac capaz de ejecutar un navegador web con soporte a HTML5 y javascript habilitado.

Instalación:

- Conectamos Safedoor con la alimentación proporcionada (5v / 3A) y conectamos el cable de red con dos posibilidades:

    - Punto a Punto. Conexión directa entre el TOE y el ordenador cliente a través del cable de red. *Nota: La mayoría de adaptadores de red modernos soportan conexiones directas con un cable de red estándar. Si el equipo es antiguo, se necesitará un cable de red cruzado*.

    - Conexión del TOE y equipo cliente a la misma red a través de switch o hub

  Para la configuración de la red el TOE ofrece tres posibilidades a través de su interfaz web:

    - Cliente DHCP: (opción por defecto)

      Obtendrá dirección IP del servidor DHCP de la red. Para facilitar la gestión de la red se incluye la dirección MAC en una etiqueta en la parte inferior del dispositivo. Esta opción no está disponible en conexiones punto a punto

    - Dirección estática

      Disponible en conexiones punto a punto y red. Se deberá proporcionar dirección IP, máscara de red y en su caso puerta de enlace y servidor DNS.

    - Servidor DHCP:

      Sólo para conexiones punto a punto, el TOE incluye un servidor DHCP que permitirá asignar automáticamente dirección IP al equipo cliente. En este caso el dispositivo estará disponible en 20.0.0.1 y el equipo cliente obtendrá una IP en el rango 20.0.0.x

  En cualquiera de los tres casos y como método de recuperación ante una configuración errónea del dispositivo o para su configuración inicial éste siempre estará disponible en la dirección 20.0.0.1.

Para acceder a esta dirección configuraremos el adaptador de red del equipo cliente con la IP estática 20.0.0.2/255.255.255.0 y abriremos un navegador web a la URL https://20.0.0.1/

4. Problemas de seguridad

4.1. Hipótesis sobre el entorno de ejecución

1. **Protección física:** El TOE está protegido en una localización segura con acceso restringido a personas confiables. En particular, el atacante no tiene acceso físico al TOE. La introducción de memorias USB en el dispositivo las llevará a cabo personal de confianza.

2. **Administrador confiable:** Se asume que el administrador del TOE actúa para garantizar la seguridad del sistema respetando las buenas prácticas y protocolos relativos a la configuración de red, seguridad criptológica, gestión de usuarios y contraseñas. El TOE no garantiza su integridad ante una configuración deficiente o maliciosa por parte del administrador.

3. **Acceso a actualizaciones:** Se asume que el TOE será actualizado por el administrador cuando esté disponible una nueva actualización de seguridad del firmware. De la misma manera se asume que el TOE tendrá acceso al servicio de actualización de firmas del antivirus.

4. **Protección de credenciales:** Se asume que el administrador y usuarios del TOE protegerán debidamente sus credenciales de acceso.

5. **Información residual:** El administrador debe garantizar que la información sensible (credenciales, certificados ..) almacenada en los TOEs descartados o eliminados del entorno operacional no pueda ser accedida por un tercero.

6. **Equipo cliente:** El equipo cliente está libre de malware y actualizado con las últimas actualizaciones de seguridad de su sistema operativo, disponiendo de uno de los siguientes navegadores web con javascript habilitado:
    - Google chrome v70.0.x o superior
    - Firefox 64.0 o superior
    - Opera 57.0 o superior
    - Internet explorer 11 o superior
    - Safari 10.0 o superior

4.2. Activos sensibles a proteger

1. **Interfaz Web**

   Es el medio de interacción principal con el usuario, basado en un servidor web embebido en el TOE al que se accederá mediante un navegador. En su bastionado se protege:

   1. Canal de comunicaciones HTTPS
   2. Credenciales de administrador y usuarios locales
   3. Control de acceso a recursos y funcionalidades en función del perfil de usuario y sesión establecida

2. **Informes de análisis**

   Cada dispositivo USB conectado al TOE y cada análisis llevado a cabo por el antivirus genera un informe de auditoría cuya integridad debe ser garantizada.

3. **Actualizaciones**

   Tanto del software del TOE como de las firmas del antivirus embebido

4. **Puertos USB**

   La función principal del TOE es identificar y anular vectores de ataque USB por lo que debe protegerse a sí mismo de estas amenazas a nivel eléctrico, hardware y software.

4.3. Descripción de las amenazas

1. **Comunicaciones de red**

   El TOE solamente debe aceptar tráfico de red dirigida a él a través del canal válido (HTTPS) e ignorar cualquier otro tráfico transversal en la red. La principal amenaza en un entorno de red es el intento por parte de un tercero malintencionado de acceder al TOE sin credenciales válidas buscando vulnerabilidades en la aplicación web.

2. **Acceso no autorizado**

Mediante distintas técnicas un agente malintencionado puede intentar adquirir una sesión válida en el TOE:

- Suplantación del TOE en la red
- Ataque Man in the Middle
- Replay de paquetes de red pertenecientes a sesiones válidas

3. **Actualizaciones de software**

   Intentos de actualización del software del TOE mediante paquetes de actualización manipulados

4. **Auditoría**

   Intentos de modificación de los informes generados por el TOE por su operativa habitual

5. **Compromiso de credenciales de administrador e información del dispositivo**

   Un manejo o almacenamiento no adecuado de información sensible (credenciales, ficheros de configuración, certificados) o el uso de contraseñas predecibles o de baja seguridad puede comprometer la operativa de TOE negando el acceso a usuario válidos y autorizando al atacante

6. **Fallo del dispositivo**

   Un atacante puede intentar provocar fallos de módulos o funcionalidades concretas para intentar intentar obtener acceso al TOE, en función de cómo éste reacciona a cada situación no habitual.

7. **Amenazas específicas USB**

   Un atacante puede intentar comprometer el TOE conectando a cualquiera de sus dos puertos dispositivos de ataque camuflados como memorias USB. Las principales amenazas son:

   a. **Familia BadUsb**

      Dispositivos USB con apariencia similar a una memoria USB creadas para llevar a cabo ataques, normalmente dirigidos, mediante distintas metodologías:

- ❏ Reprogramación: Algunos dispositivos admiten la reprogramación de firmware desde el puerto USB, lo que aprovecha el atacante para inyectar un firmware modificado capaz a su vez de infectar otros dispositivos vulnerables que se conecten al mismo puerto.

- ❏ Fake HIDs: El más conocido como producto comercial es RubberDucky, aunque existen variantes basadas entre otras en arduino o digispack, este último con un coste inferior a un euro. Estos dispositivos, una vez conectados al equipo, se identifican a nivel USB como dispositivos HID (Human Interface Devices), concretamente como teclados, y reproducen una secuencia preprogramada de pulsaciones. Existen repositorios con plantillas para diversos tipos de ataque, desde descarga y ejecución de software a exfiltración de datos sensibles. Una característica importante es que permiten seleccionar el vendorId y productId con el que identificarse ante el equipo anfitrión, lo que invalida la protección por las listas blancas de dispositivos.

- ❏ Suplantación de adaptador de red. Permite desde reemplazar los servidores DNS del sistema para ataques de spoofing a interceptar el tráfico y redirigirlo a la interfaz de red real para evitar su detección

b. **UsbKiller**:

Dispositivo comercial de apariencia similar a una memoria USB que aloja seis condensadores capaces de almacenar la energía que recibe por las líneas de alimentación USB (5V - 0.5A) y devolver ráfagas de 220-230 voltios por las líneas de datos USB.

c. **Malware**:

Desde explotación de vulnerabilidades como stuxnet a los virus tradicionales.

5. Funciones de seguridad

5.1. Especificación de las funciones de seguridad del producto

1. **Amenaza: Comunicaciones de red**

   El único destino de red accesible del TOE es el puerto 443 TCP donde acepta conexiones el servidor web, siempre utilizando HTTPS. El resto de puertos están cerrados en entrada por firewall salvo el 67 UDP, sólo activo en el caso de configuración del TOE como servidor DHCP.

   El servidor web está basado en el módulo HTTPS de node.js y embebido en el software del TOE, con la capa ssl implementada por la librería OpenSSL 1.1.0, forzando el uso de TLS 1.2. con un certificado RSA de 4096 bits con SHA-256 como algoritmo hash.

   El control de acceso a los recursos de la aplicación web se realiza mediante formulario de login (usuario / contraseña) y se realiza una verificación de acceso a cada recurso basada en roles.

2. **Acceso no autorizado**

   Se fuerza el uso de TLS 1.2 y un certificado con CA reconocida por el equipo cliente. Estas características permiten hacer frente a las amenazas de replay y renegociación de versiones anteriores del protocolo (sslv2, sslv3, tlsv1.0).

   Dado que el acceso al TOE se realiza via web, cualquier intento de suplantación de identidad del TOE o ataque Man in the Middle provocará una alerta de seguridad en el navegador web del usuario previo a la introducción de sus credenciales.

3. **Actualizaciones de software**

   Los paquetes de actualización del TOE están cifrados y firmados digitalmente para evitar la suplantación o modificación de su contenido

4. **Auditoría**

Los informes de análisis y dispositivos generados son firmados digitalmente por el TOE para evitar su modificación.

5. **Compromiso de credenciales de administrador e información del dispositivo**

   El TOE utiliza SHA256 para almacenar las credenciales de los usuarios locales.

6. **Fallo del dispositivo**

   El TOE no expone módulos susceptibles de ataque individual. El único componente independiente (antivirus) sí podría ser objeto de ataque indirecto, tanto denegando en la red su actualización como intentando corromper las actualizaciones de firmas en su descarga. En caso de fallo individual del antivirus, el TOE seguirá ofreciendo protección eléctrica y hardware y permitirá la navegación por las carpetas de las memorias USB conectadas, pero no permitirá su descarga al equipo cliente

7. **Amenazas específicas USB**

   1. **Nivel hardware**

      El TOE monitoriza la negociación a nivel USB del dispositivo introducido. Solo aceptará dispositivos puros de almacenamiento, rechazando y notificando dispositivos híbridos (Hub USB que exponen varias interfaces) y cualquier otro que no sea una memoria USB pura y se comporte como tal. Esta comprobación es continua y seguirá activa durante todo el intervalo en que el dispositivo esté conectado al TOE.

      Para ello realiza comprobaciones a distintos niveles que le permiten afrontar las amenazas conocidas y ofrecer protección ante futuras evoluciones.

      En un paso posterior, el TOE verifica que la estructura de particiones del dispositivo USB validado no presente particiones ocultas que puedan servir para exfiltrar información. En caso de detectarlas, el TOE las destacará en color rojo en la interfaz web.

   2. **Nivel eléctrico**

      El TOE incorpora protección en ambos puertos USB contra picos de tensión de alto voltaje en las líneas de datos. Esta protección es continua, estando activa desde que el usuario introduce el dispositivo USB hasta que lo retira. En caso de detección de sobretensión en la línea se genera una alerta

visible para el usuario tanto a través del LED (Rojo) del puerto USB como a través de la interfaz web.

3. **Nivel software**

El TOE incorpora un antivirus comercial que permite realizar un análisis en busca de malware en los archivos seleccionados por el usuario, siendo este un paso obligatorio antes de la descarga de ficheros al equipo cliente. En ningún caso se permitirá la ejecución de ningún fichero alojado en las memorias conectadas

6. Evaluaciones con módulos opcionales

6.1. (MEC) Listado de mecanismos criptográficos

No aplica

6.2. (MCF) Listado de mecanismos de seguridad

No aplica