Referencia: 2024-13-INF-4499-v1
Difusión: Limitada al expediente
Fecha: 14.04.2025

Creado por: CERT16
Revisado por: CALIDAD
Aprobado por: TECNICO

INFORME DE CERTIFICACIÓN

Expediente #	**2024-13**
TOE	**OPNsense Business Edition 23.10.2**
Solicitante	**NL817434306B01 - Deciso B.V**
Referencias	

[EXT-9011] 2024-03-26_2024-AE_solicitud_certificacion.zip

[EXT-9394] 2024-12-18_2024-13_ETR_v1.1

Informe de Certificación del producto OPNsense Business Edition 23.10.2, según la solicitud de referencia [EXT-9011], de fecha 17/04/2024, evaluado por el laboratorio jtsec Beyond IT Security, S.L., conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-9394], recibido el pasado 18/12/2025.

CONTENIDOS

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto OPNsense Business Edition 23.10.2.

Solicitante:	Deciso B.V.
Organismo de Certificación:	Centro Criptológico Nacional (CCN).
Laboratorio de Evaluación:	jtsec Beyond IT Security, S.L..
Tipo de Evaluación:	LINCE - Certificación Nacional Esencial de Seguridad, versión 2.0
Taxonomía según CCN-STIC-140:	No disponible.
Fecha de término de la evaluación:	15/01/2025.
Fecha de validez recomendada[1]:	26/03/2027

Todos los componentes de garantía requeridos por el tipo de evaluación LINCE presentan el veredicto de “PASA”. Por consiguiente, el laboratorio jtsec Beyond IT Security, S.L. asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador para LINCE, definidas por la norma Certificación Nacional Esencial de Seguridad, versión 2.0.

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto OPNsense Business Edition 23.10.2, se propone la resolución estimatoria de la misma.

RESUMEN DEL TOE

OPNsense Business Edition es un cortafuegos de estado basado en software. Se encarga de interconectar dos o más redes, canalizando todas las comunicaciones entre ellas a través de sí mismo para examinar cada mensaje y bloquear aquellos que no cumplan los criterios de seguridad especificados.

El TOE incluye tanto la aplicación cortafuegos como la plataforma/sistema operativo sobre el que opera. El sistema operativo subyacente, basado en FreeBSD, es un componente esencial del TOE, ya que proporciona las capacidades necesarias para la ejecución segura del TOE. Así pues, el TOE se considera una solución integrada que comprende:

1. Aplicación cortafuegos: implementa la funcionalidad de filtrado de tráfico y gestión de políticas de seguridad.

[1] Ver sección VALIDEZ DEL CERTIFICADO

2. Plataforma/Sistema Operativo: FreeBSD, configurado específicamente para soportar las operaciones de seguridad requeridas por el TOE.
3. Interfaz de gestión: Incluye tanto la interfaz de línea de comandos (CLI) como la interfaz gráfica de usuario (GUI), a través de las cuales se realiza la administración del TOE.

Aunque el TOE ofrece una amplia gama de funcionalidades adicionales, como VPN, proxy, detección de intrusos, entre otras, el alcance de la evaluación se centra en la funcionalidad de cortafuegos (filtrado de tráfico y gestión de políticas).

En este contexto, el TOE interconecta dos o más redes para que todas las comunicaciones entre estas redes pasen a través de él, con el fin de examinar cada mensaje y filtrar aquellos que no cumplan con los criterios de seguridad especificados.

El filtrado se aplica a varios niveles dentro de las capas definidas por el modelo OSI (ISO/IEC 7498-1), concretamente abordando la red (Capa 3) y el transporte (Capa 4).

ACTIVIDADES DE EVALUACIÓN

El producto se evaluó con todas las evidencias necesarias para la satisfacción del tipo de evaluación LINCE, según la norma Certificación Nacional Esencial de Seguridad, versión 2.0.

Las actividades de evaluación realizadas en el transcurso de la evaluación han sido:

- ANÁLISIS DE LA DECLARACIÓN DE SEGURIDAD
- INSTALACIÓN DEL PRODUCTO
- ANÁLISIS DE CONFORMIDAD – ANÁLISIS DE LA DOCUMENTACIÓN
- ANÁLISIS DE CONFORMIDAD –PRUEBAS FUNCIONALES
- ANÁLISIS DE VULNERABILIDADES
- PRUEBAS DE PENETRACIÓN DEL TOE

IDENTIFICACIÓN DEL TOE

Objeto de evaluación (TOE): OPNsense Business Edition 23.10.2.

Declaración de Seguridad: OPNsense Business Edition Security Target v0.8, 2024/07/29.

HIPÓTESIS Y ENTORNO DE USO

Las hipótesis restringen las condiciones sobre las cuales se garantizan las propiedades y funcionalidades de seguridad indicadas en la Declaración de Seguridad. Dichas hipótesis, se relacionan en el apartado 4.1 de la declaración de seguridad [ST].

Estas hipótesis se han aplicado durante la evaluación en la determinación de la condición de explotables de las vulnerabilidades identificadas. Por tanto, para garantizar el uso seguro del TOE, se parte de las hipótesis declaradas para su entorno de operación. En caso de que alguna de ellas no pudiera asumirse, no sería posible garantizar el funcionamiento seguro del TOE.

ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS

Las *amenazas detalladas en el* apartado 4.3 *de la declaración de seguridad [ST], no suponen un riesgo explotable para* el producto OPNsense Business Edition 23.10.2, aunque los agentes que realicen ataques tengan potencial de ataque correspondiente a moderado según lo definido en LINCE, y siempre bajo el cumplimiento de las hipótesis de uso y la correcta satisfacción de las políticas de seguridad.

Para cualquier otra amenaza no incluida en esta lista, el resultado de la evaluación de las propiedades del producto, y el correspondiente certificado, no garantizan resistencia alguna.

FUNCIONES DE SEGURIDAD

El TOE declara en el apartado 5 de la declaración de seguridad [ST] las funciones de seguridad que han sido verificadas por el CCN respecto a su cumplimiento con la Taxonomía de productos declarada con respecto de la guía CCN-STIC-140 y han sido evaluadas por el laboratorio para verificar su efectividad en el entorno operacional definido.

GUÍAS DE OPERACIÓN E INSTALACIÓN DEL TOE

El producto incluye los documentos indicados a continuación, y que deberán distribuirse y facilitarse de manera conjunta a los usuarios de la versión evaluada.

- OPNsense Business Edition Security Target v0.8, 2024/07/29.
- OPNsense Documentation versión d971b9d.

PRUEBAS DEL PRODUCTO

Para verificar la funcionalidad de seguridad declarada, el laboratorio ha desarrollado una prueba por cada una de las funciones de seguridad del producto, verificando que los resultados, así obtenidos, son consistentes con lo declarado en la Declaración de Seguridad [ST].

Adicionalmente, el laboratorio ha realizado un análisis de vulnerabilidades teniendo en cuenta las funcionalidades de seguridad declaradas en la [ST] y el nivel de resistencia a atacantes con potencial de ataque moderado tal y como se define en CCN-STIC-2002. Teniendo en cuenta las potenciales vulnerabilidades extraídas de dicho análisis, el laboratorio evaluador ha realizado pruebas de penetración para verificar la explotabilidad de las mismas en el entorno de operación declarado en [ST].

Todas las pruebas se han realizado sobre un mismo escenario de pruebas, acorde al entorno de operación, identificado en la Declaración de Seguridad [ST].

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados, y en aquellos casos en los que se presentó alguna desviación respecto de lo esperado, el evaluador ha constatado que dicha variación no supone una merma en la capacidad funcional del producto conforme a lo declarado en su Declaración de Seguridad [ST].

CONFIGURACIÓN EVALUADA

Para el funcionamiento del producto conforme a la evaluación evaluada del TOE OPNsense Business Edition 23.10.2 es necesario disponer de los componentes software que se indican en la sección 3.1 de la declaración de seguridad [ST]. Además de esto, es necesario tener en consideración las indicaciones relacionadas con el uso del TOE incluidas en la sección 2.3 de la declaración de seguridad [ST].

RESULTADOS DE LA EVALUACIÓN

El producto OPNsense Business Edition 23.10.2 ha sido evaluado en base a la Declaración de Seguridad OPNsense Business Edition Security Target v0.8, 2024/07/29.

Todas las actividades de evaluación requeridas por el tipo de evaluación LINCE presentan el veredicto de “PASA”. Por consiguiente, el laboratorio jtsec Beyond IT Security, S.L. asigna el **VEREDICTO de “PASA”** a toda la evaluación por satisfacer todas las acciones del evaluador, definidas por la norma Certificación Nacional Esencial de Seguridad, versión 2.0 para el tipo de evaluación LINCE.

RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES

A continuación, se proporcionan las recomendaciones acerca del uso seguro del producto. Estas recomendaciones han sido recopiladas a lo largo de todo el proceso de evaluación y se detallan para que sean consideradas en la utilización del producto.

- El evaluador no ha proporcionado recomendaciones o comentarios.

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto OPNsense Business Edition 23.10.2, se propone la resolución estimatoria de la misma.

El certificador adicionalmente recomienda a los usuarios finales del TOE que tengan en cuenta las siguientes recomendaciones:

- El presente certificado cubre la funcionalidad declarada en la [ST] del TOE en su versión especificada en la sección Identificación del TOE de este informe, concretamente:
    - OPNsense Business Edition 23.10.2
- Los usuarios finales del TOE deben comprobar que las hipótesis sobre el entorno de ejecución definidas en el apartado 4.1 de la declaración de seguridad [ST] son aceptables para el caso de uso esperado del TOE.

VALIDEZ DEL CERTIFICADO

Un certificado LINCE se emite indicando la versión específica del producto que fue evaluada. Si este producto evoluciona, sus nuevas versiones no serán certificadas por defecto. El proceso de “Assurance Continuity” o continuidad de la garantía [AC] se usa para facilitar el mantenimiento del certificado en versiones nuevas del producto. Este proceso es aplicable a la certificación LINCE.

Se recomienda revisar la validez del certificado a los veinticuatro meses desde su emisión. En todo momento el desarrollador podrá optar al proceso de renovación del certificado o re-certificación del mismo, según lo establecido en el procedimiento de certificación PO-005.

GLOSARIO DE TÉRMINOS

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAFÍA

Se han utilizado las siguientes normas y documentos en la evaluación del producto:

LINCE v2.0

[CCN-STIC-2001] Definición de la Certificación Nacional Esencial de Seguridad (LINCE), versión 2.0. Marzo 2022. Centro Criptológico Nacional.

[CCN-STIC-2002] Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), versión 2.0. Marzo 2022. Centro Criptológico Nacional.

[CCN-STIC-2003] Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE), versión 2.0. Marzo 2022. Centro Criptológico Nacional.

[CCN-STIC-2004] Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE), versión 2.0. Marzo 2022. Centro Criptológico Nacional.

[ST] OPNsense Business Edition Security Target v0.8, 2024/07/29.

DECLARACIÓN DE SEGURIDAD O DECLARACIÓN DE SEGURIDAD LITE (SI APLICA)

Junto con este Informe de Certificación, se dispone en el Organismo de Certificación de la Declaración de Seguridad completa de la evaluación:

- OPNsense Business Edition Security Target v0.8, 2024/07/29.