Referencia: 2020-48-INF-3403-v1
Difusión: Público
Fecha: 07.05.2021

Creado por: CERT10
Revisado por: CALIDAD
Aprobado por: TECNICO

INFORME DE CERTIFICACIÓN

Expediente #	**2020-48**
TOE	**Bittium SafeMove VPN (versions: Android (generic): 1.2.159, Android (Bittium Tough Mobile R): 2020-04-27 @ granite @ c5e05cb)**
Solicitante	**1855598-7 - Bittium SafeMove Oy**
Referencias	

[EXT-6296] Solicitud de certificación

[EXT-6430] Informe Técnico de Evaluación v1.0

Informe de Certificación del producto Bittium SafeMove VPN (versions: Android (generic): 1.2.159, Android (Bittium Tough Mobile R): 2020-04-27 @ granite @ c5e05cb), según la solicitud de referencia [EXT-6296], de fecha 26/08/2020, evaluado por el laboratorio Layakk Seguridad Informatica S.L., conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-6430], recibido el pasado 21/12/2020.

https://oc.ccn.cni.es
organismo.certificacion@cni.es

CONTENIDOS

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto Bittium SafeMove VPN (versions: Android (generic): 1.2.159, Android (Bittium Tough Mobile R): 2020-04-27 @ granite @ c5e05cb).

El Target of Evaluation (TOE) es un software cliente de VPN (red privada virtual). Es responsable de establecer un canal de comunicación de confianza (trusted channel) para comunicación TCP entre el TOE y otro dispositivo o servidor parte del entorno operacional. El canal establecido es cifrado y autenticado mutuamente, asegurando que el TOE se comunica con el servidor de VPN esperado y que el servidor se comunica con un TOE de confianza. El sistema operativo soportado por el TOE es Android o BTM-R OS dependiendo de la plataforma hardware utilizada.

Fabricante:	Bittium SafeMove Oy.
Patrocinador:	Centro Criptológico Nacional (CCN).
Organismo de Certificación:	Organismo de Certificación del Centro Criptológico Nacional (CCN).
Laboratorio de Evaluación:	Layakk Seguridad Informatica S.L.
Tipo de Evaluación:	LINCE + MEC - Certificación Nacional Esencial de Seguridad, versión 0.1
Taxonomía según CCN-STIC-140:	Redes privadas virtuales/IPSec.
Fecha de término de la evaluación:	21/12/2020.
Fecha de validez recomendada[1]:	24/04/2023.

Todos los componentes de garantía requeridos por el tipo de evaluación LINCE + MEC (Módulo de Evaluación Criptográfica) presentan el veredicto de “PASA”. Por consiguiente, el laboratorio Layakk Seguridad Informatica S.L. asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador para LINCE + MEC, definidas por la norma Certificación Nacional Esencial de Seguridad, versión 0.1.

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto Bittium SafeMove VPN (versions: Android (generic): 1.2.159, Android (Bittium Tough Mobile R): 2020-04-27 @ granite @ c5e05cb), se propone la resolución estimatoria de la misma.

[1] Ver sección VALIDEZ DEL CERTIFICADO

RESUMEN DEL TOE

El Target of Evaluation (TOE) es un software cliente de VPN (red privada virtual). Es responsable de establecer un canal de comunicación de confianza (*trusted channel*) para comunicación TCP entre el TOE y otro dispositivo o servidor parte del entorno operacional. El canal establecido es cifrado y autenticado mutuamente, asegurando que el TOE se comunica con el servidor de VPN esperado y que el servidor se comunica con un TOE de confianza. El sistema operativo soportado por el TOE es Android o BTM-R OS dependiendo de la plataforma hardware utilizada.

El TOE soporta varios algoritmos criptográficos y es compatible, por ejemplo, con la *NSA Suite B*.

A continuación, se indican los algoritmos y mecanismos criptográficos soportados:

- AES-CBC con longitud de clave de 256 bits en conformidad con NIST SP 800-38A.
- AES-GCM con longitud de clave de 256 bits en conformidad con NIST SP 800-38D.
- Servicios deterministas para generación de números aleatorios en conformidad con NIST SP 800-90A usando CTR_DRBG (AES).
- IKEv2 con NAT traversal implementado según definición RFC5996.
- Arquitectura IPSec según especificación RFC4301.
- Protocolo IPsec ESP según definición RFC 4303 usando los algoritmos criptográficos AES-GCM-256 según especificación RFC4106 y AES-CBC-256 según especificación RFC3602.
- En cuanto a los grupos Diffie-Hellman, el TOE soporta el grupo 15 según especificación RFC3526, el grupo 16 según especificación RFC3226, los grupos 19, 20, 21 según especificación RFC5903 y los grupos 28, 29, 30 según especificación RFC6954.

ACTIVIDADES DE EVALUACIÓN

El producto se evaluó con todas las evidencias necesarias para la satisfacción del tipo de evaluación LINCE, más las requeridas para el componente adicional MEC, según la norma Certificación Nacional Esencial de Seguridad, versión 0.1.

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
- EVALUACIÓN CRIPTOGRÁFICA (MEC)

IDENTIFICACIÓN DEL TOE

Objeto de evaluación (TOE): Bittium SafeMove VPN (versions: Android (generic): 1.2.159, Android (Bittium Tough Mobile R): 2020-04-27 @ granite @ c5e05cb)..

Declaración de Seguridad: Bittium SafeMove Security Target: Android VPN (versión: 1.0.10, fecha: 24/11/2020)

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 *5.2 Assumptions* 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 siguientes amenazas no suponen un riesgo explotable para el producto Bittium SafeMove VPN (versions: Android (generic): 1.2.159, Android (Bittium Tough Mobile R): 2020-04-27 @ granite @ c5e05cb), aunque los agentes que realicen ataques tengan potencial de ataque correspondiente a moderado según lo definido en Certificación Nacional Esencial de Seguridad, versión 0.1, 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.

Las amenazas cubiertas por las propiedades de seguridad del TOE se relacionan en el apartado *5.1.3 Threats* de la declaración de seguridad [ST].

FUNCIONES DE SEGURIDAD

El TOE declara en el apartado apartado *7 TOE FUNCTIONAL SECURITY* 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.

- Release Notes for Secure Suite 11.1.100, 2019-05-06.
- SafeMove Android and Windows VPN client. Preparative procedures, Version 1.0.4.
- SafeMove 11.1.100. Installation and Administration, May 6, 2019
- SafeMove Crypto IP gateway 4.11.582. Administrator's Guide, May 6, 2019.
- SafeMove CryptoIP configuration parameter guide, Version 1.0.1.
- SafeMove Management Server 11.1.100. Administrator's Guide, May 6, 2019.
- Bittium Secure Suite Administrator's Guide, Version 11.
- Bittium SafeMove Security Target: Android VPN, Version 1.0.10, 24/11/2020.

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-LINCE-002]. 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 Bittium SafeMove VPN (versions: Android (generic): 1.2.159, Android (Bittium Tough Mobile R): 2020-04-27 @ granite @ c5e05cb) es necesario disponer de los componentes software y hardware que se indican en la sección *4 OPERATIONAL ENVIRONMENT* de la declaración de seguridad [ST].

RESULTADOS DE LA EVALUACIÓN

El producto Bittium SafeMove VPN (versions: Android (generic): 1.2.159, Android (Bittium Tough Mobile R): 2020-04-27 @ granite @ c5e05cb) ha sido evaluado en base a la Declaración de Seguridad Bittium SafeMove Security Target: Android VPN (versión: 1.0.10, fecha: 24/11/2020).

Todas las actividades de evaluación requeridas por el tipo de evaluación LINCE + MEC presentan el veredicto de "PASA". Por consiguiente, el laboratorio Layakk Seguridad Informatica 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 0.1 para el tipo de evaluación LINCE + MEC.

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 laboratorio 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 Bittium SafeMove VPN (versions: Android (generic): 1.2.159, Android (Bittium Tough Mobile R): 2020-04-27 @ granite @ c5e05cb), 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:
    - Bittium SafeMove VPN (versions: Android (generic): 1.2.159, Android (BTM-R): 2020-04-27 @ granite @ c5e05cb).

- Los usuarios finales del TOE deben comprobar que las hipótesis sobre el entorno de ejecución definidas en el apartado *5.2 Assumptions* 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

BTM-R	Bittium Tough Mobile R
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:

[CCN-LINCE-001] Definición de la Certificación Nacional Esencial de Seguridad (LINCE), versión 0.1. Junio 2018. Centro Criptológico Nacional.

[CCN-LINCE-002] Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), versión 0.1. Junio 2018. Centro Criptológico Nacional.

[CCN-LINCE-003] Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE), versión 0.1. Junio 2018. Centro Criptológico Nacional.

[CCN-LINCE-004] Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE), versión 0.1. Junio 2018. Centro Criptológico Nacional.

[ST] Bittium SafeMove Security Target: Android VPN (versión: 1.0.10, fecha: 24/11/2020)

DECLARACIÓN DE SEGURIDAD

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

- Bittium SafeMove Security Target: Android VPN (versión: 1.0.10, fecha: 24/11/2020).