REF: 2010-6-INF-615 v2
Difusión: Expediente
Fecha: 01.04.2011

Creado: CERT2
Revisado: TECNICO
Aprobado: JEFEAREA

INFORME DE CERTIFICACIÓN

Expediente: 2010-6
Datos del solicitante: A82486325 RECOVERY LABS

Referencias:

[EXT-996] Solicitud de Certificación ERASEIT CORE v1.0.

[EXT-1207] ETR V2.1 ERASEIT CORE 23-07-2010 DE EPOCHE.

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, mayo 2000.

[SOGIS] European Mutual Recognition Agreement of IT Security Evaluation Certificates version 3.0, January 2010.

Informe de certificación del producto ERASEIT CORE, versión 1.0.3, según la solicitud de referencia [EXT-996], de fecha 11/05/2010, y evaluado por el laboratorio EPOCHE & ESPRI, conforme se detalla en el correspondiente informe de evaluación indicado en [EXT-1207] de acuerdo a [CCRA] y [SOGIS], recibido el pasado 23/07/2010.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

INDICE

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Resumen

Este documento constituye el Informe de Certificación para el expediente de la certificación del producto ERASEIT CORE, versión 1.0.3.

Fabricante: Recovery Labs S.A.

Patrocinador: Recovery Labs S.A.

Organismo de Certificación: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

Laboratorio de Evaluación: EPOCHE & ESPRI.

Perfil de Protección: ninguno.

Nivel de Evaluación: EAL1+ ALC_FLR.1 + ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2

Fecha de término de la evaluación: 23-07-2010.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL1+ (aumentado con ALC_FLR.1 + ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2) presentan el veredicto de “PASA”. Por consiguiente, el laboratorio EPOCHE & ESPRI asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL1, definidas por los Criterios Comunes v3.1 [CC-P3] y la Metodología de Evaluación v3.1 [CEM].

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto ERASEIT CORE v1.0.3, se propone la resolución estimatoria de la misma.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Resumen del TOE

El TOE EraseIT CORE constituye las librerías del núcleo común de la familia de software EraseIT para el borrador seguro de datos en dispositivos de almacenamiento mediante sobre-escritura de información, de la empresa Recovery Labs.

Cubre plataformas PC y discos IDE, SATA, SCSI, USB, etc. Borrado configurable según normas DoD5220.22-M, NATO Standard, US Navy, NAVSO P-5239-26 – RLL, US Air Force, AFSSI5020, Peter Gutmann patterns, etc.

Soportan auditorías de seguridad, procesos de destrucción de equipos en renovaciones de parques de informáticos, etc.

Requisitos de garantía de seguridad

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL1, más las requeridas para el componente adicional, ALC_FLR.1 + ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2, según la parte 3 de CC v3.1 r3.

Requisitos funcionales de seguridad

La funcionalidad de seguridad del producto se limita a satisfacer los requisitos funcionales, según la parte 2 de CC v3.1 r3, siguientes:

Class FDP

FDP_RIP.1 Residual information protection

FDP_RIP.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: deallocation of the resource from] the following objects: [assignment: dispositivos de almacenamiento].

Class FAU

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

FAU_GEN.1 Security audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [selection:
not specified] level of audit; and
c) [assignment: en cada operación de borrado seguro].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: método de borrado seguro utilizado, dispositivo borrado].

NOTA: el método de borrado y el dispositivo han sido seleccionados por el usuario tal y como se indica en FMT_SMF.1

Se elimina la dependencia de *FMT_STM.1 – Time stamps* debido a que el TOE no proporciona una fuente de tiempo, se utiliza una fuente externa al TOE.

Class FMT

FMT_SMF.1 - Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: seleccionar método de borrado seguro, seleccionar dispositivos sobre los que realizar la operación de borrado seguro].

Class FTP

FTP_ITC.1 – Inter-TSF trusted channel

FTP_ITC.1.1 identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [selection: aplicación cliente autorizada] to initiate communication via the trusted channel.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: todas las funciones del TOE].

Identificación

Producto: ERASEIT Core v1.0.3.

Declaración de Seguridad: Security Target for the Secure Data Erasure Software – EraseIT Core v 1.5, Julio 2010.

Perfil de Protección: ninguno.

Nivel de Evaluación: CC v3.1 r3 EAL1+ (ALC_FLR.1 + ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2).

Política de seguridad

El uso del producto ERASEIT Core, debe implementar una serie de políticas organizativas, que aseguran el cumplimiento de diferentes estándares y exigencias de seguridad.

En síntesis, se establece la necesidad de implementar políticas organizativas relativas a:

P.AUDIT	El TOE implementará una funcionalidad de auditoría que posibilitará la explotación posterior de las operaciones realizadas para su análisis en grandes flotas.
P.METHOD_SELECTION	El TOE implementará la posibilidad de seleccionar el método de borrado por parte de la aplicación cliente autorizada, para que así pueda realizar el proceso según lo especificado en la norma deseada (Ej. DoD5220.22-M, HMG Infosec Standard No:5, ...).
P.DEVICE_SELECTION	El TOE implementará la posibilidad de seleccionar por parte de la aplicación cliente autorizada los dispositivos sobre los que se realizará la operación de borrado seguro de datos.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Hipótesis y entorno de uso

La siguiente hipótesis restringe las condiciones sobre las cuales se garantizan las propiedades y funcionalidades de seguridad indicadas en la declaración de seguridad. Esta misma hipótesis se ha aplicado durante la evaluación en la determinación de la condición de explotables de las vulnerabilidades identificadas.

Para garantizar el uso seguro del TOE, se parte de la siguiente hipótesis para su entorno de operación. En caso de que no pudiera asumirse, no sería posible garantizar el funcionamiento seguro del TOE.

A.CODE

Se asume que no se ha ejecutado código por un atacante de manera previa al arranque del TOE.

Aclaraciones sobre amenazas no cubiertas

Las siguientes amenazas no suponen un riesgo explotable para el producto ERASEIT Core v1.0.3, aunque los agentes que realicen ataques tengan potencial de ataque correspondiente a “Basic” de EAL1, 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.

Amenaza cubierta:

T.DATA_RECOVERY	Un usuario con acceso al disco tras la realización del proceso de borrado pueda realizar una recuperación de los datos originales.
T.NOT_AUTHORIZED	Una aplicación cliente no autorizada pueda comunicarse con el TOE.
T.NOT_PRIVACY	Una aplicación cliente no autorizada pueda conocer los datos transmitidos en la comunicación entre el TOE y una aplicación cliente autorizada.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Funcionalidad del entorno.

El producto requiere de la colaboración del entorno para la cobertura de algunos objetivos del problema de seguridad definido.

El único objetivo que se debe cubrir por el entorno de uso del producto es el siguiente:

OE.CODE

El entorno debe garantizar que ningún atacante pueda ejecutar código de manera previa al arranque del TOE.

Arquitectura

Arquitectura Lógica:

EraseIT Core es una aplicación que se carga durante el arranque del sistema desde diversos medios de distribución (CD/DVD, USB, red, etc). Integra su propio sistema operativo, por lo que elimina cualquier dependencia con éste y aumenta la compatibilidad del producto.

Software para el borrado seguro de datos almacenados en dispositivos de almacenamiento. Es una aplicación utilizada como núcleo de borrado en aplicaciones clientes de borrado seguro. Se trata de software destinado al borrado seguro de datos almacenados en dispositivos de almacenamiento. El borrado seguro de los datos se realiza mediante la sobre-escritura de la información. La aplicación base se ejecuta sobre una plataforma PC-compatible y utiliza las controladoras de discos IDE, SATA, SCSI, USB para el acceso a la información y la sobreescritura de los discos seleccionados por el usuario. Sobre las unidades de lectura asociadas a los dispositivos de almacenamiento, como en el caso de las unidades USB tipo U3, NO se realiza la operación de borrado seguro. El método de borrado es configurable por la aplicación cliente, posibilitando al usuario la realización del mismo según lo especificado en las normas DoD5220.22-M, HMG Infosec Standard No:5, NATO standard, US Navy, NAVSO P-5239-26 – RLL, US Air Force, AFSSI5020, Peter Gutmann patterns, etc.

El proceso de operación de borrado queda registrado mediante una auditoría que al finalizar la operación será almacenada en el mismo dispositivo de almacenamiento y podrá ser exportado a la aplicación cliente.

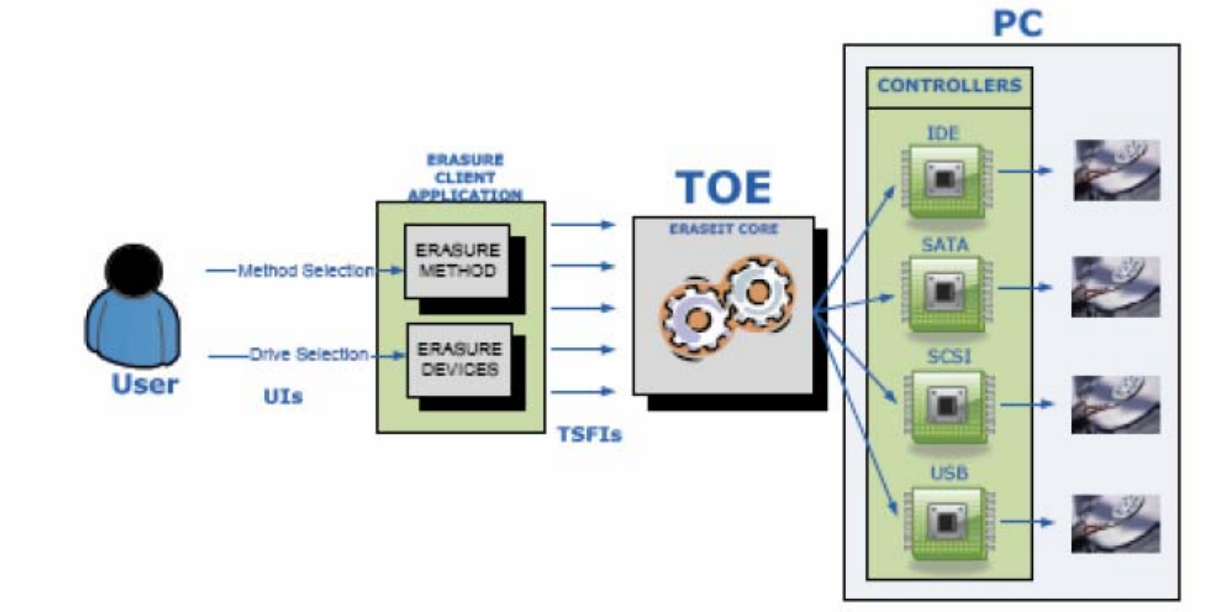
ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Funcionalidades	*Ámbito*	*Coms*
Borrado seguro de datos	T	
Selección de dispositivos a borrar	T	
Selección de método de borrado (DoD5220.22-M, HMG Infosec Standard No:5,…)	T	
Auditoría de proceso	T	
Cifrado del informe de borrado	X	
Verificación horaria a través del servidor NIST	X	
Gestión de licencias de uso	X	
Panel de control web para la gestión de borrados	X	Add-on

T - En el TOE
X - Excluido del TOE

Arquitectura Física:

EraseIt Core es una aplicación software y por lo tanto todo el hardware/firmware queda excluido desde el punto de vista de componentes externos.



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Documentos

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

- Security Target for the Secure Data Erasure Software – EraseIT Core v 1.5, Julio 2010.

- EraseIt Core Manual de desarrollador v 1.0.5, 9 julio 2010

Pruebas del producto

El evaluador ha seleccionado un subconjunto de pruebas y una estrategia apropiada para el TOE entregado por el fabricante. La documentación de la especificación funcional del TOE describe el comportamiento de las TSFIs y el evaluador ha aplicado esa información a la hora de desarrollar sus pruebas.

Para ello se ha tenido en cuenta:

- Trascendencia de los interfaces

- Tipos de interfaces

- Número de interfaces

Para la selección de las pruebas se han utilizado como criterios: la búsqueda de parámetros críticos en la interacción con las TSFIs, realización de pruebas exhaustivas en las TSFIs de mayor importancia y sospechas de mal comportamiento de las TSFIs ante determinados parámetros de entrada.

También se han realizado pruebas con parámetros de las TSFIs que pudieran tener especial relevancia en el mantenimiento de la seguridad del TOE.

El fabricante ha realizado pruebas para todas las funciones de seguridad. Todos las pruebas ha sido realizados por el fabricante en sus instalaciones con resultado satisfactorio.

Configuración evaluada

Las pruebas de penetración y funcionales de borrado se han realizado sobre los dispositivos que el fabricante declara que soporta y con el siguiente entorno de pruebas:

− Procesador: Intel Celeron D 336, 2800 MHz (21 x 133)

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- Placa Base: ASRock 775i65G
- Chipset de la placa base: Intel Springdale-G i865G
- RAM: 1024 MB
- BIOS: AMI P.300 (20/03/07)

El producto declara soportar el borrado de los siguientes dispositivos:

- **Controladoras**:
  - Controladora SCSI: PCS SCSI Adaptec AHA-2940UW
  - Controladora IDE: Intel(R) 82801EB - 24D1
  - Controladora USB: Intel 82801EB ICH5 - USB Controller [A-2/A-3]

- **Discos**:
  - Disco SCSI: SEAGATE ST39103LW SCSI Disk Device (9 GB, 10000 RPM, Ultra2 SCSI) - LS568113000010161ZJX
  - Disco SATA: SEAGATE ST96812AS (60 GB, 5400 RPM, SATA) - 5PJ01493
  - Disco USB: SEAGATE ST3802110A USB Device (80 GB, 7200 RPM, Ultra-ATA/100)
  - Disco IDE: SEAGATE ST380215A (80 GB, 7200 RPM, Ultra-ATA/100) - QZ6XX52
  - Disco USB Extraible: USB Flash Memory USB Device (486 MB, USB)

Resultados de la Evaluación

El producto ERASEIT Core v1.0.3 ha sido evaluado frente a la declaración de seguridad “Security Target for the Secure Data Erasure Software – EraseIT Core v1.5, Julio 2010”.

Todos los componentes de garantía requeridos por el nivel de evaluación **EAL1+** (aumentado con ALC_FLR.1 + ASE_SPD.1, ASE_OBJ.2, ASE_REQ.2) presentan el veredicto de “PASA”. Por consiguiente, el laboratorio EPOCHE & ESPRI asigna el **VEREDICTO de “PASA”** a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL1+, definidas por los Criterios Comunes [CC-P3] y la Metodología de Evaluación [CEM] en su versión 3.1 r3.

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 fabricante ha implementado un mecanismo para impedir el falseo de la marca de borrado de los dispositivos. Sin embargo, la marca podría llegar a ser falseada.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Por lo tanto, se recomienda utilizar además, otras medidas para saber si un dispositivo determinado ha sido borrado con anterioridad.

o A pesar de que el TOE arranca desde CD, no existe una cadena de confianza que permita un arranque seguro, por lo tanto, se recomienda no utilizar el TOE en un PC que haya sido comprometido con anterioridad.

o No se debe utilizar el TOE para realizar el borrado sobre las unidades de lectura asociadas a los dispositivos de almacenamiento, como en el caso de las unidades USB tipo U3; puesto que no se realizará la operación de borrado seguro.

Recomendaciones del certificador

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto ERASEIT Core v1.0.3, se propone la resolución estimatoria de la misma.

Glosario de términos

CCN	Centro Criptológico Nacional
HW	HardWare
SW	SoftWare
IT	Information Technology
PC	Personal Computer
TOE	Target of Evaluation

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Bibliografía

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

[CC_P1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, Version 3.1, r3, July 2009.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, r3, July 2009.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, r3, July 2009.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 3.1, r3, July 2009.

Declaración de seguridad

Conjuntamente con este informe de certificación, se dispone en el Organismo de Certificación de la declaración de seguridad completa de la evaluación:

"Security Target for the Secure Data Erasure Software – EraseIT Core v1.5, Julio 2010".

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es