centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de referencia para productos de seguridad TIC - Anexo B.4: Herramientas de actualización de sistemas

Diciembre 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.12.27 13:13:40 +01'00'

NIPO: 083-19-053-9.

Fecha de Edición: diciembre 2019
ISDEFE ha participado en el desarrollo del presente documento.

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Herramientas de Actualización de Sistemas** para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC), publicado por el CCN.
2. Estos requisitos representan las capacidades de seguridad mínimas que cualquier producto dentro de esta familia debe implementar para un determinado caso de uso, independientemente del fabricante y la tecnología, con el fin de proporcionar un nivel mínimo de confianza y considerarse objetivamente cualificado desde el punto de vista de la seguridad para ser empleado en los sistemas de información del sector público a las que sea de aplicación el Esquema Nacional de Seguridad (ENS). Estos requisitos aportan mecanismos enfocados a reducir vulnerabilidades y contrarrestar amenazas, fundamentalmente de carácter técnico, aunque también pueden ser de naturaleza física o procedimental.
3. Además, la aplicación de estos criterios permitirá:
   - Que se establezcan unas características mínimas de seguridad que sirvan de referencia a los **fabricantes** a la hora de desarrollar nuevos productos STIC.
   - Que los **organismos responsables de la adquisición** dispongan de evaluaciones completas, consistentes y técnicamente adecuadas, que permitan contrastar la eficacia y proporcionar información no sesgada acerca de los servicios de seguridad que ofrecen dichos productos.
   - Que los **usuarios finales** posean una guía que facilite el despliegue y garantice el uso apropiado del producto desde el punto de vista de la seguridad.
4. Por lo tanto, los productos catalogados dentro de la familia **Herramientas de Actualización de Sistemas** conforme a la taxonomía definida por el Centro Criptológico Nacional, serán susceptibles de ser evaluados usando como referencia este documento.
5. En el caso de productos multipropósito, queda fuera del alcance de este documento cualquier otra funcionalidad de seguridad proporcionada, más allá de la especificada para esta familia en la sección siguiente. Dichos productos podrían optar a ser incluidos de manera adicional como Productos Cualificados en otra(s) familia(s) del CPSTIC si cumpliesen los RFS correspondientes.

2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS

2.1 FUNCIONALIDAD

6. Los productos asociados a esta familia están orientados fundamentalmente a la actualización del sistema. Permiten actualizar los componentes software para añadir nuevas funcionalidades o corregir fallos o vulnerabilidades existentes.
7. Las funciones básicas de seguridad que proporcionan esta familia de productos son las siguientes:
   - Despliegue de correcciones publicadas para las vulnerabilidades conocidas.
   - Distribución de nuevas funcionalidades o mejoras respecto a las versiones anteriores.
   - Administración del ciclo de gestión de las actualizaciones (orígenes, destinatarios, planificación, mecanismos, etc.).

2.2 CASOS DE USO

En el caso de los productos de esta familia se contemplan los siguientes casos de uso.

2.2.1. CASO DE USO 1 – ACTUALIZACIONES *OFFLINE*

8. En el caso de redes o dispositivos que permanezcan aislados por requisitos de seguridad, la actualización no puede realizarse estableciendo canales de comunicación directos con las fuentes que proporcionan los recursos para la actualización.
9. En estos casos, en primer lugar, se procederá a la descarga, comprobación y aprobación de las actualizaciones. Un usuario autorizado importará a la herramienta de actualización en la red que se encuentra aislada. Finalmente, se instalarán los paquetes de actualizaciones ejecutando los instaladores necesarios.
10. Se pueden dar dos aproximaciones al respecto:
    - Los agentes atienden a las peticiones de actualización iniciadas por parte del servidor. En esta situación a herramienta determinará las acciones que se realizarán en el sistema. Por lo tanto, en este caso no hay intervención por parte del usuario.
    - Los clientes se conectarán periódicamente al servidor centralizado para ver si existen nuevas actualizaciones y en caso afirmativo las descargará. Existe la posibilidad de ofrecer al usuario la posibilidad de elegir el momento de su aplicación.

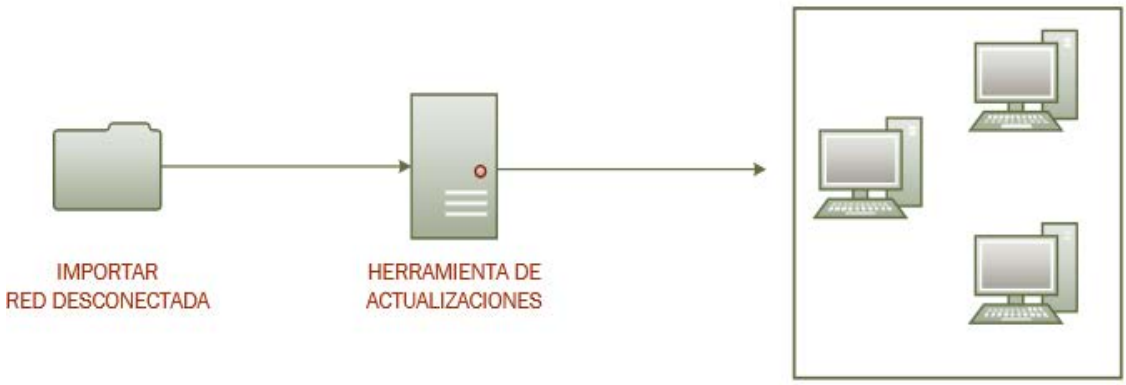

Figura 1. Ejemplo de Caso de Uso 1: Actualizaciones Offline

2.2.2. CASO DE USO 2 – ACTUALIZACIONES *ONLINE*

11. El producto verifica periódicamente de manera manual o automática si las versiones del *software/firmware*[1] soportados son las últimas disponibles. Seguidamente, procedería a la descarga del paquete de actualizaciones de manera online, mediante la descarga desde una fuente de confianza. Posteriormente la herramienta de actualización desplegará los paquetes ejecutando los instaladores necesarios.

Figura 2. Ejemplo de Caso de Uso 2: Actualizaciones Online

2.3 ENTORNO DE USO

12. Este tipo de dispositivos son de uso generalizado en cualquier tipo de ámbito, en particular en el caso de redes con gran cantidad de equipos a administrar, debido a su trascendencia para el correcto mantenimiento de las redes informáticas y de comunicaciones, tanto en el caso de redes desplegadas en ámbitos empresariales como en el sector público.
13. Para la utilización en condiciones óptimas de seguridad, es necesaria su integración en un entorno operacional que cumple las siguientes condiciones mínimas de protección:

[1]Firmware funciona como el nexo de unión entre las instrucciones (software) que llegan al dispositivo desde el exterior y las diversas partes electrónicas (hardware)

- **Protección física**. El producto deberá instalarse en un área donde el acceso sólo sea posible para el personal autorizado y con condiciones ambientales adecuadas.
- **Plataforma segura**: El producto se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución sobre el que se utilice.
- **Administración confiable**. El Administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la empresa/administración. Por ello se asume que dicha persona estará capacitada, formada y carecerá de cualquier intención dañina al administrar el producto.
- **Actualizaciones periódicas**. El producto será puesto al día conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
- **Protección de las comunicaciones.** Deberán habilitarse los mecanismos necesarios que permitan una comunicación segura, así como las redes a las que estos se conecten bajo el control de la organización.
- **Protección de la información**. El entorno debe proteger y garantizar el uso del sistema de gestión de base de datos, donde se almacena la información, además de que sea confiable.
- **Política de seguridad de la información.** La política de seguridad deberá recoger el conjunto de principios, la organización y los procedimientos impuestos por una organización para hacer frente a sus necesidades de seguridad de la información, incluyendo el uso de las TIC.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

14. Este tipo de productos se presenta en formato **Software** que se instala en dispositivos Hardware con las funcionalidades estrictamente necesarias para cumplir su finalidad y acotadas al servicio específico que presten.
15. Adicionalmente, suele ser habitual que en las máquinas y dispositivos a los que suministran las actualizaciones se despliegue una aplicación **Software** (agente) que controla los dispositivos conectados en la red.
16. En caso de ofrecer funcionalidades adicionales a las definidas en la sección 2, éstas quedan fuera del alcance analizado, debiendo ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

17. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TI (Tecnologías de la Información).

18. En el ámbito de CC se elaboran unos perfiles de seguridad que definen, para un dominio o categoría de productos, un conjunto de objetivos y requisitos de seguridad, tanto funcionales como de evaluación, independientes de la implantación.

19. Los productos dentro de esta familia deberán cumplir con los SFR (*Security Functional Requirements*) que se especifican en el siguiente perfil de protección certificado de acuerdo a la norma *Common Criteria,* junto con los restantes requisitos fundamentales de seguridad recogidos en la sección 4:

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Application Software[2].	1.2	25/04/2016	NIAP

Tabla 1. Perfil de protección

20. El nivel de confianza EAL (*Evaluation Assurance Level*) con el que deben ser evaluados los requisitos exigidos para esta familia será:

    - **El determinado por el perfil de protección** para aquellos SFR incluidos en el perfil exigido cuando los productos se encuentren certificados contra éste.
    - **EAL2 o superior** para los RFS adicionales que no encuentren incluidos dentro del perfil.
    - **EAL2 o superior** en el caso en el que el producto no se encuentre certificado contra el perfil.

[2] http://www.commoncriteriaportal.org:80/files/epfiles/pp_app_v1.2.pdf

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

21. Los recursos a proteger mediante el uso de estos productos, así como para su correcto funcionamiento, incluyen:

    - Paquetes de actualización, almacenados o en tránsito, recibidos de la fuente confiable y a distribuir.
    - Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos.
    - Información sensible que pueda almacenar el dispositivo en su almacenamiento interno.
    - Datos de configuración del producto y de auditoría generados por éste.

3.2 AMENAZAS

22. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente serían:

    - **Ataque a la red.** Un atacante, que acceda al canal de comunicación, puede modificar las comunicaciones entre los distintos módulos del producto.
    - **Monitorización del tráfico.** Un atacante, desde dentro o desde fuera de la red, consigue acceder a información intercambiada entre los distintos módulos de la aplicación.
    - **Ataque local.** Un atacante puede actuar a través de Software ejecutado en la misma plataforma de computación donde se ejecuta el producto. Los atacantes podrían modificar de forma dañina los ficheros o comunicaciones que utiliza el producto.
    - **Acceso físico.** Un atacante podía acceder a información sensible almacenada en el sistema.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

23. A continuación, se recogen los requisitos fundamentales de seguridad que deben cumplir los productos que quieran optar a la inclusión en el CPSTIC en esta familia.

4.1 PERFIL DE PROTECCIÓN

24. **REQ. 1** El producto debe cumplir con los SFR (*Security Functional Requirements*) que se especifican en el siguiente perfil de protección certificado de acuerdo a la norma *Common Criteria*:

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Application Software	1.2	25/04/2016	NIAP

Tabla 2. Perfil de protección

25. **REQ. 2** En caso de que el producto no esté certificado contra el perfil indicado, la declaración de seguridad deberá contener al menos los SFR (*Security Functional Requirements*) de éste con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

4.2 REQUISITOS CRIPTOGRÁFICOS

26. **REQ. 3** Todos los algoritmos de cifrado simétrico, asimétrico, protocolos de acuerdo de clave y funciones resumen que utilice el producto deberán encontrarse dentro de los acreditados por el CCN para su uso en el ENS. El listado de dichos algoritmos se encuentra recogido en la CCN-STIC-807 (Categoría ALTA).

4.3 CONTROL DE LOS FLUJOS DE INFORMACIÓN

27. **REQ. 4** El producto debe permitir el alta, baja y modificación de las fuentes confiables desde las que se importarán los paquetes de actualización.

28. **REQ. 5** El producto debe permitir el alta, baja y modificación de los sistemas cliente a los que distribuir las actualizaciones, incluyendo información relativa a su identificación inequívoca y al software/firmware a actualizar.

29. **REQ. 6** Cada paquete descargado de la fuente de confianza requiere la autorización de un usuario autorizado para su despliegue en el sistema cliente.

30. **REQ. 7** El producto debe registrar y permitir la consulta, para cada sistema cliente afectado, el estado de los paquetes distribuidos, indicando la versión del paquete y resultado del despliegue.
31. **REQ. 8** El producto debe permitir gestionar la desinstalación de los paquetes distribuidos (de forma individual o colectiva).
32. **REQ. 9** El producto debe permitir la importación y verificación de los paquetes de actualización, ya sea de fuentes confiables online como de mecanismos de transferencia de datos offline.

4.4 REGISTROS AUDITORIA

33. **REQ. 10** Se debe proporcionar un medio para almacenar los eventos relacionados con la seguridad, de forma que permita interpretarse por un usuario.
34. **REQ. 11** Los registros de auditoría contendrán al menos la siguiente información: fecha y hora del evento, tipo de evento identificado, resultado del evento, usuario que produce el evento.
35. **REQ. 12** Se registrarán en la auditoria los siguientes eventos:
    a. Iniciar o detener la auditoria de la aplicación
    b. Cambios en el grupo de usuario que tiene el rol de administrador.
    c. Utilización por parte del usuario de los mecanismos de autenticación.
    d. Cualquier utilización de los mecanismos de autenticación del producto
    e. Todas las decisiones en cuanto a las peticiones en el intercambio de información entre la red interna y externa.
    f. Cambio de hora o fecha.
    g. Cambios de la configuración del producto
36. **REQ. 13** Los registros de auditoría, no podrán modificarse por ningún usuario.
37. **REQ. 14** Sólo podrán leer los registros de auditoría los usuarios autorizados.
38. **REQ. 15** Los administradores serán los únicos usuarios que puedan borrar registros de auditoría.

5. ABREVIATURAS

CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
EAL	*Evaluation Assurance Level*
ENS	*Esquema Nacional de Seguridad*
NIAP	*National Information Assurance Partnership*
RFS	Requisitos Fundamentales de Seguridad
SFR	*Security Functional Requirements*