Servicio de soporte de vulnerabilidades

Abstract: la detección de vulnerabilidades en las tecnologías de la información es una actividad de especial relevancia por su directa implicación en la seguridad de los dispositivos y equipos informáticos. Asimismo, resulta imprescindible notificar dichas vulnerabilidades en tiempo oportuno a organizaciones y usuarios para facilitar la respuesta y toma de decisiones. Bajo esta premisa, y con el objetivo de continuar fortaleciendo la ciberseguridad nacional, el CCN-CERT ofrece un nuevo servicio de análisis, notificación y seguimiento de vulnerabilidades.

Contenido:

1 INTRODUCCIÓN

El presente documento busca dar a conocer el procedimiento establecido para poner en marcha un servicio de análisis, notificación y seguimiento de las vulnerabilidades más críticas que impacten en productos de tecnologías de la información ampliamente empleados por los organismos públicos que conforman la comunidad del CCN-CERT.

2 OBJETIVO Y ALCANCE

El objetivo del presente procedimiento consiste en aportar un valor añadido a los organismos adscritos a los servicios del CCN-CERT, que complemente a los sistemas de alerta temprana, avisos y publicaciones de vulnerabilidades que el CCN-CERT viene poniendo a disposición de su comunidad de referencia.

Para ello, se establecen las siguientes actividades:

- Trabajar en la recopilación y clasificación de las nuevas vulnerabilidades que aparecen en el mercado.
- Realizar un análisis teórico y en laboratorio, cuando sea posible, de aquellas vulnerabilidades que por su criticidad se consideren, necesidad de mitigación o afectación en los productos desplegados en los organismos públicos adscritos al servicio.

- Generación de "abstracts" para difusión de aquellas vulnerabilidades que se hayan considerado, detallando aspectos como la afectación y vector de ataque, potencialidad de este, recomendaciones y buenas prácticas para protegerse de los mismos, así como sus diferentes actualizaciones.
- Seguimiento de la evolución de la vulnerabilidad en Internet, alertando a los organismos ante cambios en la criticidad, aparición de parches, nuevas recomendaciones, constancia de explotaciones activas, etc.

3 CARACTERÍSTICAS DEL SERVICIO

3.1 Flujo del servicio

El servicio de monitorización de vulnerabilidades seguirá el siguiente flujo de funcionamiento:

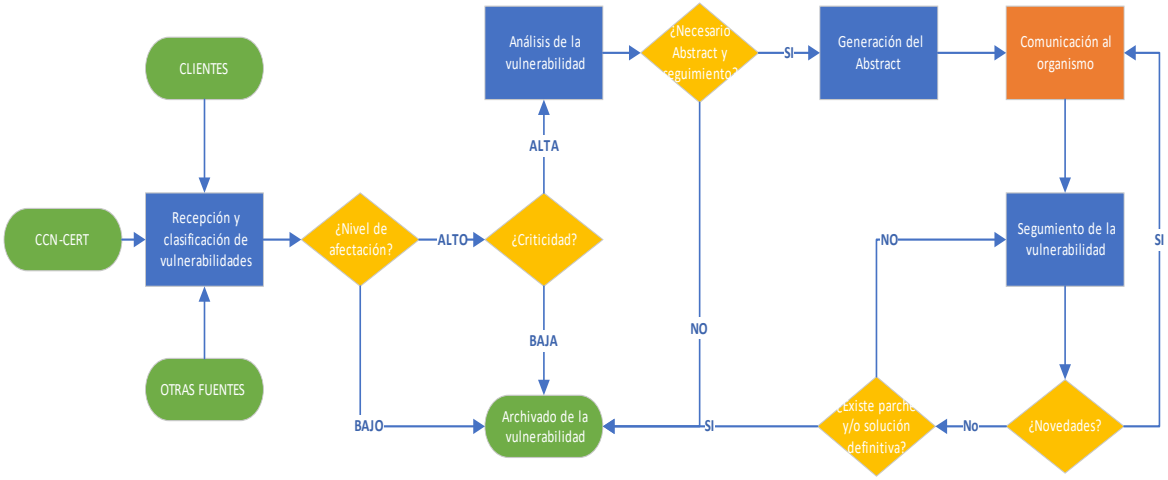

Figura 1.- Flujograma servicio de soporte y monitorización de vulnerabilidades

3.2 Recepción y clasificación de vulnerabilidades

Como primera fase del servicio, se realiza una clasificación de las vulnerabilidades notificadas por el propio CCN-CERT como fuente principal, sin renunciar a otras fuentes, provenientes de otros CERT, blogs de seguridad o las propias notificaciones de los fabricantes y organismos.

Para un correcto análisis del nivel de afectación utilizado para clasificar la vulnerabilidad, se utilizará la experiencia de los gestores de vulnerabilidades y la información proporcionada por los organismos y el CCN-CERT. En un primer nivel de madurez del servicio, se contemplarán únicamente los componentes más críticos y extendidos en los organismos, tales como:

- Sistemas operativos en servidores y puestos de trabajo, incluyendo plataformas móviles.
- Servidores, tecnologías y *frameworks* más utilizados en el desarrollo de aplicaciones.

- Sistemas perimetrales como *firewalls* o balanceadores.
- Aplicaciones más utilizadas.
- Sistemas de acceso remoto a las infraestructuras.

El otro factor más relevante en la clasificación de las vulnerabilidades es el **nivel de criticidad**, para el que se utilizará el estándar *Common Vulnerability Scoring System Version 3.0 (CVSS3.0)* para aquellas vulnerabilidades a las que se les haya asignado un CVE y realizado el cálculo CVSS3.0. Inicialmente, se considerarán únicamente aquellas vulnerabilidades que superen el 9 en esta escala, y siempre que no exista una solución definitiva, como un parche de seguridad del fabricante en cuyo caso raramente requerirá de un análisis adicional.

Para aquellas vulnerabilidades que no tengan asignado un CVE y CVSS, se utilizará como referencia la clasificación de criticidad que el anunciante (fabricante o investigador) de la vulnerabilidad proporcione, junto al criterio técnico de los gestores de vulnerabilidades, considerando únicamente las definidas como críticas.

3.3 Análisis de la vulnerabilidad

Para aquellas vulnerabilidades cuyo nivel de afectación sea ALTO y su criticidad ALTA, se realizará un análisis de esta, revisando la documentación existente en Internet sobre las mismas y las pruebas de concepto que puedan existir.

Cuando sea posible realizar un análisis en laboratorio, se tendrá en consideración con el objetivo de realizar las siguientes acciones:

- Validar posibles mecanismos para identificar si se está afectado.
- Evaluar el posible impacto de la vulnerabilidad, siempre que existan pruebas de concepto o la suficiente documentación de cómo explotarla.
- Evaluar las medidas de mitigación y las posibles consecuencias de su aplicación.

El nivel de análisis de cada vulnerabilidad será muy variable, dependiendo de la información pública de la misma, que varía notablemente de quien es el anunciante de la misma.

3.4 Generación del Abstract

Una vez realizado el análisis y si se considera necesario, se generará un “abstract” donde se recogerá la siguiente información:

- Antecedentes sobre el problema si existieran.
- Afectación y vector de ataque.
- Potencialidad del ataque.
- Conclusiones y recomendaciones.

3.5 Comunicación al organismo

El “abstract” se enviará a los organismos adscritos al servicio, pudiendo ser publicado asimismo dentro de los comunicados que el CCN-CERT genera habitualmente.

Para casos específicos, se establecerá una única dirección de correo electrónico (*soporte_acreditacion@ccn.cni.es*), que será utilizada para la comunicación mediante esta vía. Asimismo, será la cuenta de correo establecida como punto de contacto y soporte a la que los organismos adscritos podrán dirigirse para aclarar dudas o solicitar ayuda.

Del mismo modo, se generará una carpeta en la solución LORETO donde se almacenará el “abstract” y toda la información relevante asociada. Esta misma carpeta servirá para almacenar toda la información que se genere durante su seguimiento. A corto/medio plazo toda esta información se registrará en una instancia de ANA de acceso público, donde se podrá realizar un seguimiento de la evolución de las vulnerabilidades.

3.6 Seguimiento de la vulnerabilidad

El servicio incluye un seguimiento de la vulnerabilidad, entendiéndolo como la vigilancia de su evolución a partir de la información disponible en Internet y en las fuentes utilizadas, no realizando un seguimiento de cómo se está mitigando o parcheando en los organismos adscritos al servicio.

En caso de constatar variaciones en la evolución de la vulnerabilidad, se notificará a los organismos:

- Aparición del parche de seguridad que solventa el problema.
- Constatación de la explotación activa de dicha vulnerabilidad.
- Variaciones en la clasificación de la vulnerabilidad.
- Nuevas formas o vías para mitigar el problema en caso de no existir parche.
- Nuevas formas de comprobar la afectación o la aparición de nuevos productos afectados.
- Etc.

Estas actualizaciones se notificarán vía correo electrónico a los organismos y toda la información asociada se actualizará en el repositorio establecido en LORETO, así como en ANA.

Cuando se haga oficial el parche de una vulnerabilidad o la solución definitiva a la misma, se considerará cerrada la vulnerabilidad y su seguimiento. En caso de que los sistemas de vigilancia del CCN-CERT detecten campañas de explotación de la vulnerabilidad, se podrá volver a abrir el caso si se considera necesario, para su seguimiento y posible análisis.

ESTADO VULNERABILIDAD	viernes, 8 de mayo 2020		
Identificación	**0-click MAIL IOS**	**Nivel de Criticidad**	**CRÍTICO**
Afectación	**Apple Mail (IOS 6 - IOS 13)**	**Fecha de descubimiento**	**20/04/2020**
Estado	**Activa, a la espera de parche**	**Días activa**	**19**
CVSS	No disponible	**Código CCN**	**10049Av40-20**
Prueba de concepto	No disponible	**CVE**	**No disponible**
Referencia	https://blog.zecops.com/vulnerabilities/youve-got-0-click-mail/		
Descripción	Explotación de una vulnerabilidad que podría estar afectando a los dispositivos con sistema operativo tipo iOS, fundamentalmente iPhone e iPad. Dicha vulnerabilidad afectaría a sus aplicaciones fundamentales: la aplicación de MAIL que presenta dichos dispositivos y que es bastante empleada al ser nativa al permitir conectar a diversas plataformas como MS Exchange Server, Office 365 o Gmail		
Último Abstract	https://www.ccn-cert.cni.es/seguridad-al-dia/avisos-ccn-cert/10049-ccn-cert-av-40-20-analisis-de-la-vulnerabilidad-en-ios-mail-recomendaciones-y-buenas-practicas.html		

NIVEL DE AFECTACIÓN			
Sistema operativo	☒	Correo	☑
Base de Datos	☒	Servidor de Ficheros	☒
Servidor Web	☒	Firewall	☒
Puesto Cliente	☑	Dispositivo Movil	☑

BÚSQUEDAS	Resultados	Fecha
Blogs especializados	Nada relevante	8-may.-20
Pruebas de concepto/exploits	Nada relevante	8-may.-20
Rredes Sociales	Tweet de los investigadores que descubrieron la vulnerabilidad: https://twitter.com/ZecOps/status/1256028858022674432?s=20	8-may.-20
Fuentes oficiales del fabricante	Nada relevante	8-may.-20

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.05.10 01:27:54 +02'00'