



CYBSEC S.A.
www.cybsec.com

CYBSEC Política de Publicación de Vulnerabilidades

La presente política detalla el procedimiento llevado adelante por CYBSEC en referencia a publicación de vulnerabilidades de seguridad. La intención detrás de esta política es permitir a las partes involucradas (vendedores de software, investigadores y consumidores) actuar sobre la vulnerabilidad de manera tal que se mitiguen los riesgos al mínimo posible.

Esta política establece las guías generales acatadas por el equipo de investigación una vez descubierta una vulnerabilidad de seguridad; detallando los pasos seguidos por el equipo de investigación y la interacción con el vendedor de software.

Los objetivos de la misma son los siguientes:

- Educar a todas las partes involucradas, proveyendo a la comunidad de seguridad informática con la información necesaria para reproducir, estudiar y verificar la vulnerabilidad en cuestión.
- Minimizar los riesgos asociados para todas las partes involucradas.
- Proveer al vendedor del software con la información necesaria para desarrollar una solución a la vulnerabilidad en cuestión.
- Contribuir al campo de investigación en seguridad informática, mediante la publicación de código “prueba de concepto” (del inglés, proof of concept) para ayudar al desarrollo de técnicas y productos diseñados para mitigar y prevenir la vulnerabilidades en el software.

Pasos involucrados en el proceso de publicación de vulnerabilidades

La presente sección esboza los pasos básicos llevados adelante por el equipo de investigación de CYBSEC durante la publicación de una vulnerabilidad de seguridad. Dependiendo de la situación específica puede resultar que no sean acatados todos los pasos, esto depende principalmente del esfuerzo demostrado por el vendedor del producto en el desarrollo de una solución y la validación de la existencia de la vulnerabilidad.

A continuación se enumera los distintos pasos, con una descripción detallada de los mismos en la siguiente sección.

1. Descubrimiento: CYBSEC detecta la vulnerabilidad de seguridad.
2. Notificación del Vendedor: El vendedor es notificado de la vulnerabilidad y es asistido por el equipo de investigación con la información técnica disponible.
3. Corroboración por parte del Vendedor: El vendedor debería proseguir con la reproducción de la vulnerabilidad para cerciorar los hallazgos de CYBSEC.
4. Desarrollo de una Solución: El vendedor debería, una vez que el problema es diagnosticado correctamente y aislado, desarrollar un parche (del inglés, patch) para problema en cuestión. La solución puede ser probada, antes del lanzamiento de la misma, por CYBSEC para asegurar que el problema haya sido resuelto.
5. Publicación del Aviso de Seguridad: El Aviso de Seguridad (en inglés, Security Advisory) se lanzará en forma pública y abierta de forma coordinada con el vendedor. El vendedor puede proceder luego a publicar su propio aviso en relación a la disponibilidad de una solución.

Detalle de los pasos involucrados en el proceso de publicación de vulnerabilidades

A continuación se detalla el procedimiento de cada uno de los pasos mencionados previamente.

Descubrimiento:

Una vez que la vulnerabilidad ha sido descubierta, la misma es estudiada hasta que pueda ser totalmente reproducida. Luego, un documento interno sobre la vulnerabilidad es producido. El mismo incluye la siguiente información:

- Descripción de la vulnerabilidad descubierta y los riesgos potencial que implica.
- Información técnica, lo más detallada posible, sobre los pasos necesarios para reproducir la misma.
- Código “prueba de concepto”, de es posible.

Notificación del Vendedor:

Una vez que el documento ha producido el documento mencionado anteriormente el vendedor es contactado (vía e-mail o teléfono, dependiendo del vendedor). Se le envía una copia del documento interno. Este primer contacto es referido de aquí en adelante como “fecha inicial de notificación”. El documento enviado al vendedor hace referencia a este documento.

Si el vendedor no provee un contacto de seguridad, CYBSEC probará con los caminos de contactos oficiales del contacto provistos por el vendedor. Si no se brinda ninguno, el aviso de seguridad se publica.

Luego de un periodo de tres (3) días de la fecha inicial de notificación, si el vendedor no ha confirmado que recibió el contacto previo, se intenta recontactar al vendedor.

Luego de un periodo de siete (7) días de la fecha inicial de notificación, si el vendedor no ha confirmado que recibió el contacto previo, confirmando que han leído el documento y proponen una agenda para la resolución de la vulnerabilidad, se hace público el aviso de seguridad.

Corroboración por parte del Vendedor:

Esta fase del procedimiento es considerada únicamente por cuestiones de concretar tiempos. Los detalles de esta fase están en las manos del vendedor. Sin embargo, proveemos las siguientes recomendaciones para producir una solución confiable al problema.

El vendedor debería seguir alguna variación de los pasos siguientes:

- Reproducir la vulnerabilidad.
- Determinar si la vulnerabilidad ya ha sido resuelta o ya era conocida, en cuyo caso deberá informar esta situación a CYBSEC.
- Determinar si otros productos del vendedor (basado en el que posee la vulnerabilidad o con funcionalidad similar) tiene la misma vulnerabilidad.
- Aislar el segmento de código fuente involucrado.
- Corregir la vulnerabilidad.

El vendedor se debería contactar con CYBSEC cada semana durante esta fase para proveer comentarios actualizados sobre la situación. De no ocurrir esto, CYBSEC publicará el aviso de seguridad.

Desarrollo de una Solución:

Esta fase involucra principalmente al vendedor, ya que durante la misma el vendedor debería resolver la vulnerabilidad creando un parche o proveyendo de un "workaround" (solución alternativa) para la misma.

El vendedor podrá solicitar extensiones de tiempo de ser necesario, justificando el tiempo requerido.

El vendedor deberá probar el parche, previo a su publicación, para asegurar que no afectará instalaciones funcionales. Se alienta a que el vendedor solicite la colaboración de CYBSEC para la etapa de prueba del parche desarrollado.

Se alienta al vendedor a resolver el problema dentro de un periodo de treinta (30) días desde el contacto inicial de notificación. Si CYBSEC percibe que el vendedor requiere de más tiempo y cree que el vendedor le ha dado la importancia

necesaria, se le dará más tiempo al vendedor antes de la publicación. Si esta nos es la situación luego de cuarenta y cinco (45) días de la notificación inicial, CYBSEC hará público el aviso de seguridad.

Publicación del Aviso de Seguridad:

A través de la cooperación con el vendedor se fija una fecha para la publicación del aviso de seguridad. La fecha se fijará de manera tal que se encuentre disponible el parche tan pronto como se haya publicado el aviso. La fecha de publicación únicamente sufrirá alteraciones por uno de los siguientes motivos:

- Un tercero hace pública la vulnerabilidad; por lo tanto CYBSEC publicará su aviso para ayudar a proveer soluciones alternativas (“workarounds”) a la comunidad.
- Si el vendedor solicita una extensión de tiempo y CYBSEC considera que ha sido solicitada en buena fe.
- Si el vendedor no puede llegar a un acuerdo con CYBSEC con respecto a la fecha de publicación, CYBSEC publicará el aviso en quince (15) días.

Si el día de la fecha de publicación, el vendedor no ha resuelto la vulnerabilidad y no se ha contactado con CYBSEC, se publicará el aviso.

La siguiente información se encuentra en un aviso de seguridad.

- **Advisory Name (Nombre del Aviso):** Un nombre asignado a la vulnerabilidad por CYBSEC.
- **Vulnerability Class (Clase de Vulnerabilidad):** La clase de la vulnerabilidad.
- **Release Date (Fecha de Publicación):** Fecha de publicación.
- **Affected Applications (Aplicaciones Afectadas):** Productos del vendedor en los cuales la vulnerabilidad ha sido detectada y probada exitosamente.
- **Not Affected Applications (Aplicaciones No Afectadas):** Otras versiones de los productos mencionados en el punto anterior donde la vulnerabilidad no está presente.
- **Affected Platforms (Plataformas Afectadas):** Plataformas en las cuales los productos vulnerables han sido probados exitosamente con respecto a la existencia de la vulnerabilidad.
- **Not Affected Platforms (Plataformas No Afectadas):** Plataformas donde los productos vulnerables son, en principio, no afectados por dicha vulnerabilidad.
- **Local / Remote (Local / Remoto):** Si la vulnerabilidad puede ser explotada localmente o remotamente.
- **Severity (Severidad):** Riesgos acarreados por la presencia de la vulnerabilidad.
- **Author (Autor):** Autor de la vulnerabilidad.

- **Vendor Status (Estado según el Vendedor):** El estado de la vulnerabilidad según si el vendedor está al tanto de la misma y en tal caso si ha proporcionado un parche.
- **CVE Candidate:** CVE número de candidato.
- **Reference to Vulnerability Disclosure Policy (Referencia a la Política de Publicación de Vulnerabilidades):** Link al presente documento.
- **Overview (Explicación General):** Descripción del producto involucrada y de la vulnerabilidad detectada.
- **Vulnerability Description (Descripción Técnica):** Detalles técnicos de la vulnerabilidad.
- **Exploit:** Código fuente “prueba de concepto” para verificar la presencia de la vulnerabilidad.
- **Solutions (Soluciones):** Posibles soluciones, incluyendo links a información provista por el vendedor (parches, etc.) y soluciones alternativas.
- **Vendor Response (Respuesta del Vendedor):** Una descripción de la respuesta del vendedor con respecto a cómo fue manejada la vulnerabilidad.