Este compromiso voluntario se centra en los productos y servicios de software empresarial, lo que incluye el software local, los servicios en la nube y el software como servicio (SaaS, por sus siglas en inglés). Los productos físicos, como los dispositivos de Internet de las cosas (IoT, por sus siglas en inglés) y los productos de consumo, no se incluyen en este compromiso, aunque se invita a las empresas que deseen demostrar su progreso en estos ámbitos a que lo hagan. Al participar en el compromiso, los fabricantes de software se comprometen a esforzarse de buena fe para alcanzar los objetivos que se enumeran a continuación durante el próximo año. Si un fabricante de software consigue un progreso medible hacia un objetivo, deberá documentar de forma pública cómo lo ha logrado en el plazo de un año desde la firma del compromiso. En caso de que el fabricante de software no pueda lograr un progreso medible, se le recomienda que, en el plazo de un año desde la firma del compromiso, comparta con la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA, por sus siglas en inglés) de qué manera ha trabajado para alcanzar el objetivo y los desafíos a los que se ha enfrentado. Y, siguiendo el espíritu de transparencia radical, se recomienda al fabricante que documente su enfoque de forma pública para que otros puedan aprender. Este compromiso es voluntario y no es legalmente vinculante.

La estructura del compromiso contiene siete objetivos. Cada objetivo incluye los criterios básicos que los fabricantes se comprometen a cumplir, además del contexto y de los ejemplos de enfoques para lograr el objetivo y demostrar el progreso medible. Para permitir una variedad de enfoques, los fabricantes de software que participan en el compromiso son libres de decidir cuál es la mejor manera de cumplir y demostrar los criterios básicos de cada objetivo. La demostración del progreso medible en todos los productos del fabricante puede adquirir diversas formas, como tomar medidas para todos los productos o elegir un conjunto de productos para abordar primero y publicar una hoja de ruta para otros productos.

La CISA reconoce y celebra a los fabricantes de software que ya cumplen o superan estos objetivos. En caso de que alguno de ellos ya cumpla o supere un objetivo, deberá describir de forma pública de qué manera lo hace. En estos casos, la CISA valora positivamente los esfuerzos adicionales para sobrepasar los objetivos del compromiso.

Este compromiso se propone complementar y ampliar las prácticas recomendadas establecidas sobre la seguridad del software, entre las que se incluyen las desarrolladas por la CISA, el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) y otras agencias federales, así como las prácticas recomendadas internacionales y del sector. La CISA continúa fomentando la adopción de medidas complementarias que promuevan una postura de seguridad desde el diseño.

AUTENTICACIÓN MULTIFACTOR (MFA)

OBJETIVO: En el plazo de un año desde la firma del compromiso, demostrar las medidas adoptadas para aumentar de forma medible el uso de la autenticación multifactor en todos los productos del fabricante.

CONTEXTO: La autenticación multifactor es la mejor defensa contra los ataques relacionados con contraseñas, como la reutilización de credenciales y el robo de contraseñas. Se ha demostrado que cualquier forma de autenticación multifactor (MFA, por sus siglas en inglés) reduce considerablemente el éxito de este tipo de ataques, y las formas más seguras de MFA, como la MFA resistente a la suplantación de identidad, ofrecen aún más protección contra los ataques dirigidos.
Los fabricantes deben intentar aumentar la inscripción en la MFA entre sus clientes de forma generalizada, haciendo hincapié, si es posible, en la adopción de una MFA resistente a la suplantación de identidad y en el aumento de la inscripción por parte de los administradores.

Nota: Otras formas de autenticación resistentes a la suplantación de identidad, como las claves de paso, también cumplen esta definición aunque sean la única forma de autenticación.

Ejemplos de enfoques para lograr este objetivo:

- Habilitar la MFA por defecto para usuarios y administradores (p. ej., solicitar a los usuarios y administradores que configuren la MFA tras el primer registro).
- Implementar recomendaciones de seguridad en los productos para incentivar a los usuarios a activar la MFA. Esto podría incluir, por ejemplo, avisos o anuncios intersticiales que notifiquen a los usuarios o administradores que la MFA no está activada o que sugieran que los administradores activen la MFA resistente a la suplantación de identidad.
- Admitir el inicio de sesión único (SSO, por sus siglas en inglés) basado en estándares en la versión básica del producto, lo que permite a los clientes configurarlo con su propio proveedor de identidad que admita la MFA.

Ejemplos de demostración de progreso medible:

- Publicar estadísticas globales de adopción de la MFA con el tiempo, desglosadas por tipo de usuario (p. ej., usuario estándar, administrador) y tipo de MFA (p. ej., SMS, contraseña de un solo uso y duración definida [TOTP, por sus siglas en inglés], FIDO2).
- Publicar un artículo de blog en el que se describan los progresos medibles conseguidos, como los casos en los que la MFA se ha activado por defecto, y en el que se señalen los obstáculos existentes.
- Participar en foros para impulsar estándares a largo plazo relacionados con la MFA o la autenticación y demostrar cómo generarán un progreso medible hacia este objetivo.

Nota: Para este objetivo, los fabricantes podrían demostrar un progreso medible mediante resultados del comportamiento de los clientes (como un cambio en el uso de la MFA en todos sus productos) o mediante cambios en el producto en sí (como la activación de la MFA por defecto).

CONTRASEÑAS PREDETERMINADAS

OBJETIVO: En el plazo de un año a partir de la firma del compromiso, demostrar un progreso medible hacia la reducción de las contraseñas predeterminadas en todos los productos de los fabricantes.

CONTEXTO: Las contraseñas predeterminadas, que la CISA define como contraseñas compartidas de forma universal que están presentes por defecto en un producto, siguen permitiendo que se produzcan ciberataques perjudiciales. El objetivo de este punto es reducir el porcentaje de contraseñas predeterminadas explotables para disminuir los ataques, prestando especial atención a los productos conectados a Internet. Las contraseñas predeterminadas deben reemplazarse por mecanismos de autenticación más seguros, como se detalla en los ejemplos siguientes (y, preferiblemente, por la MFA, como se mencionó anteriormente). Al finalizar el aprovisionamiento, el cliente es el único que debería tener sus credenciales de autenticación.

Ejemplos de enfoques para lograr este objetivo:

- Facilitar contraseñas iniciales aleatorias y únicas para cada instancia del producto.
- Solicitar al usuario que instala el producto que cree una contraseña segura al inicio del proceso de instalación.
- Facilitar contraseñas de configuración de tiempo limitado que se desactiven al finalizar el proceso de configuración y requieran la configuración de una contraseña segura (o enfoques de autenticación más seguros, como la MFA resistente a la suplantación de identidad).
- Solicitar acceso físico para la configuración inicial y la especificación de credenciales únicas de cada instancia.
- Organizar campañas u ofrecer actualizaciones para cambiar las contraseñas predeterminadas de las implementaciones existentes por mecanismos de autenticación más seguros.

Ejemplos de demostración de progreso medible:

- Publicar un artículo de blog en el que se describa cómo el fabricante está sustituyendo (o ya ha eliminado) las contraseñas predeterminadas en varias líneas de productos.
- Publicar la cantidad de productos que tienen contraseñas predeterminadas en el transcurso del tiempo.
- Publicar detalles sobre la cantidad de clientes que han cambiado sus contraseñas predeterminadas por mecanismos de autenticación más seguros.

REDUCCIÓN DE CLASES ENTERAS DE VULNERABILIDAD

OBJETIVO: En el plazo de un año desde la firma del compromiso, demostrar las medidas adoptadas para permitir una reducción significativa y medible de la prevalencia de una o más clases de vulnerabilidad en todos los productos del fabricante.

CONTEXTO: La gran mayoría de las vulnerabilidades explotadas en la actualidad corresponden a clases de vulnerabilidades que, a menudo, pueden prevenirse a escala. Algunos ejemplos son la inyección de lenguaje de consulta estructurado (SQL, por sus siglas en inglés), el scripting entre sitios y las vulnerabilidades de seguridad de memoria, como se explica a continuación. Una forma eficaz en que los fabricantes de software pueden disminuir el riesgo para sus clientes es mediante la reducción de las clases de vulnerabilidades a escala en todos sus productos. Los fabricantes de software pueden elegir una o varias clases de vulnerabilidad en las que se comprometen a trabajar para reducirlas en el transcurso del año. Para obtener más información sobre las clases de vulnerabilidad que pueden prevenirse a escala, consulte la serie Alerta de seguridad desde el diseño de la CISA.

Ejemplos de enfoques para lograr este objetivo:

- Aplicar de forma constante el uso de consultas con parámetros para evitar los ataques de inyección de SQL.
- Adoptar marcos de plantillas web con protección integrada contra vulnerabilidades de scripting entre sitios.
- Elaborar una hoja de ruta segura para la memoria a fin de comenzar a utilizar lenguajes seguros para la memoria con un enfoque prioritario y escribir nuevos productos en estos lenguajes.
- Facilitar valores predeterminados seguros a los desarrolladores, por ejemplo, ofreciendo componentes básicos de funciones y bibliotecas seguras que imposibiliten (o dificulten considerablemente) la introducción de una determinada clase de vulnerabilidad.

Ejemplos de demostración de progreso medible:

- Publicar un blog sobre cómo el fabricante ha trabajado en el último año para reducir de forma significativa la prevalencia de una o más clases de vulnerabilidad. Esto puede incluir el análisis de la causa raíz (enumeración de debilidades comunes [CWE, por sus siglas en inglés]) de las vulnerabilidades y exposiciones comunes (CVE, por sus siglas en inglés) con el tiempo en los productos del fabricante. La CISA señala que alcanzar con éxito este objetivo puede suponer un aumento a corto plazo de las CVE mientras el fabricante intenta reducir esa clase de vulnerabilidad. Si dicha clase de vulnerabilidad se reduce a largo plazo, debería considerarse un logro.
- Publicar una hoja de ruta de seguridad de la memoria o una hoja de ruta similar para otras clases de vulnerabilidad.

PARCHES DE SEGURIDAD

OBJETIVO: En el plazo de un año desde la firma del compromiso, demostrar las medidas adoptadas para aumentar de forma medible la instalación de parches de seguridad por parte de los clientes.

CONTEXTO: De acuerdo con el primer principio de seguridad desde el diseño, los fabricantes de software deben responsabilizarse de los resultados de seguridad de sus clientes, incluso

después de que los productos se hayan enviado. Además de eliminar clases enteras de vulnerabilidades en su origen, como se ha mencionado anteriormente, los fabricantes de software tienen la posibilidad de facilitar a los clientes la instalación de parches de seguridad, por ejemplo, ofreciendo compatibilidad con parches de seguridad de forma generalizada a los usuarios y habilitando la funcionalidad para llevar a cabo actualizaciones automáticas.

Ejemplos de enfoques para lograr este objetivo:

- Proporcionar la funcionalidad para permitir la instalación automática de parches de software cuando sea posible y habilitar esta funcionalidad por defecto, cuando corresponda.
- Ofrecer compatibilidad con parches de seguridad de forma generalizada a los clientes.
- En los casos en que los productos ya no sean compatibles con los parches de seguridad y hayan llegado al final de su vida útil, comunicar con claridad la vida útil prevista en el momento de la venta y, cuando el producto cumpla ese plazo, comunicarlo claramente a los clientes e invertir en capacidades de aprovisionamiento para facilitar la transición de los clientes a las versiones compatibles.
- En el caso de los productos en la nube o de SaaS, aplicar parches para que la responsabilidad no recaiga en los clientes.

Ejemplos de demostración de progreso medible:

- Publicar estadísticas globales de adopción de parches por producto con el tiempo (p. ej., el porcentaje de usuarios que utilizan distintas versiones de cada producto).
- Publicar un artículo de blog en el que se muestren las medidas adoptadas para fomentar una mayor implementación de parches de seguridad por parte de los usuarios o que reduzcan de alguna otra forma la responsabilidad de los clientes de aplicar los parches.

Nota: Para este objetivo, los fabricantes podrían demostrar un progreso medible mediante resultados del comportamiento de los clientes (como un cambio en el porcentaje de usuarios de varias versiones de un producto) o mediante cambios en el producto en sí (como la funcionalidad para aplicar parches de software automáticos).

POLÍTICA DE DIVULGACIÓN DE VULNERABILIDADES

OBJETIVO: En el plazo de un año a partir de la firma del compromiso, publicar una política de divulgación de vulnerabilidades (VDP, por sus siglas en inglés) que autorice las pruebas por parte de miembros del público en productos ofrecidos por el fabricante, se comprometa a no recomendar ni emprender acciones legales contra cualquier persona que realice esfuerzos de buena fe para seguir la VDP, ofrezca un canal claro para informar las vulnerabilidades y permita la divulgación pública de vulnerabilidades

de acuerdo con las prácticas recomendadas de divulgación coordinada de vulnerabilidades y los estándares internacionales.

CONTEXTO: La divulgación coordinada de vulnerabilidades ha surgido como una norma de colaboración con los investigadores de seguridad que beneficia a ambas partes. Los fabricantes de software se benefician de recibir ayuda de la comunidad de investigación en seguridad que les puede permitir proteger mejor sus productos. Los investigadores de seguridad reciben autorización para realizar pruebas según la política, además de un canal claro para informar vulnerabilidades. Para ver ejemplos de la política de divulgación de vulnerabilidades y el lenguaje de puerto seguro, consulte la plantilla de política de divulgación de vulnerabilidades de la CISA y la herramienta de creación de políticas de Disclose.io.

Nota: Debido al carácter específico de este punto, no se incluyen ejemplos del logro de este objetivo.

Ejemplos de demostración de progreso:

- Publicar una política pública de divulgación de vulnerabilidades según los criterios anteriores.
- Publicar una descripción legible por máquina de la política de divulgación de vulnerabilidades (p. ej., un archivo security.txt) para posibilitar el descubrimiento por parte de los investigadores.
- Publicar artículos de blog en los que se repasen los hallazgos y las conclusiones obtenidas de la política de divulgación de vulnerabilidades.

CVE

OBJETIVO: En el plazo de un año desde la firma del compromiso, demostrar transparencia en el informe de vulnerabilidades mediante la inclusión de campos precisos de enumeración de debilidades comunes (CWE) y enumeración de plataformas comunes (CPE, por sus siglas en inglés) en cada registro de vulnerabilidades y exposiciones comunes (CVE) de los productos del fabricante. Además, emitir CVE de manera oportuna para, como mínimo, todas las vulnerabilidades críticas o de alto impacto (ya sean descubiertas de manera interna o por terceros) que requieran acciones por parte de un cliente para aplicar parches o que tengan pruebas de explotación activa.

Aunque no es obligatorio para lograr este objetivo, se anima a las empresas a sobrepasar el objetivo presentando CVE para otras vulnerabilidades que no cumplan estos criterios por los motivos que se describen a continuación. También se recomienda a las empresas que exploren otras formas de mejorar sus registros de CVE para ayudar a los clientes a responder mejor a las vulnerabilidades.

CONTEXTO: Además de actuar como medio normalizado para comunicar las medidas que deben adoptar los clientes para protegerse contra las vulnerabilidades, los registros de CVE oportunos, correctos y completos permiten la transparencia pública de las tendencias de vulnerabilidad a lo largo del tiempo. Esto beneficia tanto a las empresas individuales y a sus

clientes como a la industria del software en general, ya que permite a los desarrolladores de software comprender mejor las clases de vulnerabilidades más urgentes con el paso del tiempo. El informe oportuno de las CVE, en particular de aquellas con una explotación activa, es esencial para garantizar que los clientes sean conscientes de las medidas que deben tomar. La CISA advierte que no se debe interpretar la presencia de CVE como un signo negativo, ya que el número de CVE informadas puede aumentar a corto plazo a medida que un fabricante de software aplica los principios de seguridad desde el diseño: un informe más exhaustivo de las CVE beneficia a todos.

Nota: Debido al carácter específico de este punto, no se incluyen ejemplos del logro de este objetivo.

Ejemplos de demostración de progreso:

- Publicar los campos de CWE y CPE en cada registro de CVE de los productos del fabricante.
- Describir de forma pública la política del fabricante para cuando se emite un informe de CVE.

PRUEBAS DE INTRUSIONES

OBJETIVO: En el plazo de un año desde la firma del compromiso, demostrar un aumento medible de la capacidad de los clientes para reunir pruebas de intrusiones de ciberseguridad que afecten a los productos del fabricante.

CONTEXTO: Es fundamental que las organizaciones puedan detectar los incidentes de ciberseguridad que se hayan producido y comprender lo que ha sucedido. Los fabricantes de software pueden permitir que sus clientes lo hagan facilitándoles herramientas y capacidades para reunir pruebas de las intrusiones, como los registros de auditoría del cliente. De este modo, los fabricantes de software incorporan el principio de seguridad desde el diseño que consiste en responsabilizarse de los resultados de seguridad de sus clientes.

Ejemplos de enfoques para lograr este objetivo:

- Como parte de la versión básica de un producto, facilitar registros relacionados con áreas como las siguientes:
    - cambios en la configuración o lectura de los ajustes de configuración;
    - flujos de red e identidad (p. ej., inicio de sesión y creación de tokens), si corresponde;
    - acceso a datos o creación de datos relevantes para la empresa.
- En el caso de los proveedores de servicios en la nube y los productos de SaaS, conservar los registros durante un plazo determinado (p. ej., 6 meses) sin costo adicional.

- En los casos en que un producto no admite la recopilación de este tipo de registros, el fabricante publica detalles sobre cómo los clientes pueden supervisar el producto y responder a los incidentes de ciberseguridad que afectan a este.

Ejemplos de demostración de progreso medible:

- Documentar las políticas del fabricante sobre el suministro de registros y su conservación (en el caso de los proveedores de nube).
- Publicar una hoja de ruta para añadir o mejorar las capacidades de registro de los productos que actualmente no admiten la recopilación de determinados tipos de registros.