GUÍA PARA EL REPORTE DE VULNERABILIDADES PARA LOS ADMINISTRADORES ELECTORALES EN ESTADOS UNIDOS

Conozca a los Investigadores de Seguridad

Los Estados Unidos se expresan a través de sus elecciones. Los ciudadanos esperan la misma velocidad, seguridad y precisión en la votación que esperan en sus comunicaciones. Incluso cuando emitimos una papeleta en un lugar de votación, los funcionarios electorales confían en docenas de sistemas de datos electrónicos para llevar las boletas correctas a cada votante registrado y garantizar que se cuenten con precisión.

Al igual que otros sistemas electrónicos, el riesgo para los sistemas electorales se puede manejar de manera efectiva, pero existen vulnerabilidades. Los administradores electorales deben saber que la comunidad de investigación de seguridad cibernética puede ayudar a garantizar que estos sistemas sean seguros para que las opciones del público votante puedan escucharse claramente. Esta Guía ofrece una orientación paso a paso para los administradores electorales que buscan establecer un programa exitoso de reporte de vulnerabilidades.

- **Como administradores electorales, usted ya confía en los miembros del público con tareas electorales extremadamente delicadas, desde el registro de votantes hasta el registro de votación/ controles de identidad y el conteo de votos.**

- **Las elecciones libres y justas son un componente clave de nuestra democracia, y todos tenemos un papel que desempeñar para mantenerlas a salvo de interferencias.**

- **Los investigadores de seguridad cibernética que siguen las políticas de reporte de vulnerabilidades pueden ayudarlo a mantener las elecciones seguras.**

Para aprovechar los aportes de los investigadores de seguridad cibernética, deberá:

1. Identificar claramente los sistemas en los que les permitiría realizar pruebas.
2. Detallar la naturaleza de las pruebas permitidas por escrito.
3. Definir un punto de contacto.
4. Tener recursos (incluido el personal) para investigar y solucionar los problemas que reportan al tiempo que los mantiene informados.

¿Quiénes son los investigadores de ciberseguridad?

- **Si bien sus motivaciones y capacidades son diversas, los investigadores de seguridad legítimos son personas que prueban sitios web, sistemas, software y hardware en busca de vulnerabilidades que:**
  - Puedan explotarse para hacerlos funcionar de una manera que su operador no pretendía.
  - Puedan comprometer la confidencialidad, integridad o disponibilidad de la información.
  - Puedan ayudar al investigador a comprender cómo funcionan o están diseñados los sitios web, los sistemas, el software o los productos de hardware.
- **Los investigadores de ciberseguridad tienen varios objetivos: "presumir benevolencia" (consulte la guía CERT-CC) cuando los investigadores cumplen con las políticas de prueba autorizadas.**
  - Muchos investigadores son profesionales que buscan hacer avanzar la informática como disciplina académica, crear negocios para una empresa de seguridad cibernética o ganar recompensas por errores.
  - Otros son aficionados que se ofrecen como voluntarios para ayudar a las organizaciones a evitar el abuso.
  - Algunas son personas que simplemente ven un sitio web o un producto y actúan porque les preocupa.

- **Los investigadores de ciberseguridad a menudo usan las mismas tácticas que un atacante malicioso con el objetivo de identificar vulnerabilidades que los atacantes maliciosos podrían explotar.**
- **Los investigadores de seguridad legítimos se diferencian de los atacantes malintencionados en que los investigadores éticos informan de sus hallazgos para ayudar a solucionarlos y no tienen la intención de utilizar la información con fines ilícitos.**
    - Los defensores de la divulgación coordinada de vulnerabilidades a menudo citan estas normas éticas:
        - Intentar ayudar a la entidad afectada a corregir las vulnerabilidades antes de divulgarlas públicamente.
        - No revelar a terceros los datos a los que accedió en el curso de las pruebas.
        - Publicar hallazgos para ayudar a otros a solucionar el mismo problema.

¿Qué pueden hacer los investigadores de ciberseguridad para ayudarme?

- **Encuentrar e informar los problemas de seguridad antes de que se produzca una manipulación.**
- **Conectarlo con otras personas en la comunidad de investigación que podrían ofrecerle ayuda.**
- **Tipos de problemas:**
    - Configuraciones incorrectas de red y dispositivos (que a menudo hacen que los datos sean accesibles de forma remota). Esto incluye datos confidenciales accesibles fuera de un firewall y adaptadores de red habilitados en dispositivos aislados.
    - Vulnerabilidades en el nivel de aplicación o controles de seguridad deficientes, incluida la configuración predeterminada o sin contraseña para acceder a bases de datos, o saneamiento de datos deficiente en formularios web.
    - Dispositivos que contienen vulnerabilidades de seguridad conocidas.
- **Recuerde que si alguien reporta un problema de seguridad en su red, un actor malicioso también puede encontrarlo.**

TABLA DE CONTENIDOS

PASO 1

Identificar los sistemas que aceptan pruebas de seguridad y aquellos donde están restringidos

- **Cada uno de los miles de estados y jurisdicciones electorales locales en Estados Unidos es un poco diferente, pero llevan a cabo funciones básicas similares que a menudo reciben algún tipo de apoyo electrónico:**

- Registro de votantes y verificación del registro de votantes
- Mantener a los votantes informados sobre dónde, cuándo y cómo votar
- Distribución de las boletas apropiadas a las personas/ lugares correctos
- Bienvenida a los votantes y (ocasionalmente) validación de identificación
- Tabulación y reporte de votos
- Auditorías posteriores a las elecciones
- Asignación de votantes registrados a distritos y lugares de votación, creación de listas de votación
- Manejo de trabajadores electorales
- Configuración de máquinas de votación y tabulación /dispositivos de almacenamiento de boletas
- ¡Votación!
- Reporte durante la noche de elecciones

CONSIDERE EL SISTEMA ELECTRÓNICO UTILIZADO EN CADA ETAPA Y CÓMO FUNCIONAN EN CONJUNTO

Identifique (en privado) los sistemas que deben conectarse a la **Internet pública**

Identifique (en privado) los sistemas que solo deben conectarse **entre sí**

Identifique (en privado) los sistemas que deben ser **aislados de la red**

- **Los investigadores de seguridad a menudo descubren que estos elementos están conectados de forma inesperada, o que los inventarios de activos de las organizaciones están incompletos (con protecciones desiguales para los sistemas).**

- **Considere si su organización electoral utiliza proveedores de servicios administrados, contratistas de software como servicio u otras plataformas de infraestructura electrónica para cumplir con las funciones principales:**

    - Los sistemas de terceros y sus interconexiones con los sistemas propios de su organización son parte importante del riesgo para sus operaciones.

        - Los proveedores de tecnología electoral en contrato con los gobiernos estatales y locales son responsables de muchas partes críticas de los sistemas electorales cuyo diseño y código requieren la certificación previa de la Comisión de Asistencia Electoral de EE. UU. antes de su uso en elecciones federales.

        - Si bien los gobiernos estatales y locales tienen la autoridad legal para designar los sistemas y las redes que poseen para realizar pruebas de vulnerabilidad con el fin de reducir el riesgo de sus misiones, el requisito de certificación para los sistemas electorales puede significar que la expansión de las políticas públicas de divulgación y prueba de vulnerabilidades a los sistemas operados bajo contrato requiera una planificación previa significativa.

    - Asegúrese de tener la autoridad legal para autorizar pruebas de seguridad en las redes o dispositivos propiedad de entidades de terceros antes de incluirlos en sus protocolos.

        - Las organizaciones electorales pueden negociar estos términos en sus contratos con los proveedores.

        - Su organización puede acercarse a sus proveedores para expresar su voluntad de autorizar las pruebas si el contrato existente no es claro en este punto.

        - Algunos proveedores de uso común han publicado políticas sobre las pruebas de seguridad de sus servicios.

        - Si el proveedor no está dispuesto a autorizar pruebas de seguridad pública, asegúrese de que los rangos de IP, los subdominios y otros sistemas relevantes estén claramente fuera del alcance en sus protocolos.

- **Ideentifique los sistemas, dominios y rangos de IP que usted aceptaría probar para detectar vulnerabilidades de seguridad.**

    - Si un recurso está diseñado para el acceso público (por ejemplo, su sitio web), la prueba es simple.
        - Muchas políticas de divulgación de vulnerabilidades simplemente enumeran dominios y subdominios, a veces con un operador comodín (es decir, * .elections.state.gov).

        - Los sistemas específicos de estos dominios todavía se pueden identificar como fuera de alcance en sus protocolos.

    - Los investigadores también pueden informarle cuándo elementos que nunca deben ser accesibles ¡son accesibles!

    - Los intentos de mapear su red o encontrar datos de votantes en servicios en la nube son más complejos.

PASO 2 Redactar una Política de Reporte de Vulnerabilidades fácil de leer (Ver Apéndice III)

- **Una Política de divulgación de vulnerabilidad pública permite que cada administrador electoral establezca reglas para las pruebas autorizadas, creando una guía para su relación con los investigadores de seguridad.**
- **Las organizaciones que buscan autorizar las pruebas de sus sistemas conectados a Internet generalmente publican una Política de Divulgación de Vulnerabilidades en un sitio web público que se puede ubicar fácilmente desde la página de inicio de la organización o mediante una búsqueda en la red.**
- **Considere que los investigadores de seguridad tienen diferentes motivaciones en su trabajo, lo que los llevará a esperar cosas diferentes de usted.**

- **Las políticas de divulgación de vulnerabilidades incluyen, como mínimo, estos elementos básicos:**

1. Cuáles sistemas, rangos de IP, sitios y/o elementos de almacenamiento de datos están autorizados para pruebas.
2. Cuáles tipos de pruebas están permitidas o prohibidas.
3. Una declaración explícita que prohíba la divulgación de cualquier información de identificación personal o datos no públicos a terceros.
4. Una descripción de cómo enviar informes de vulnerabilidad, que debe incluir:
    a. Cómo/dónde enviar un informe (es decir, una dirección de correo electrónico o un servicio web seguro) y una clave de cifrado para el correo electrónico.
    b. Una solicitud de información (conocida como “prueba de concepto”) necesaria para encontrar y analizar la vulnerabilidad.
        i. Una descripción de la vulnerabilidad y su impacto técnico.
        ii. El dispositivo físico o ubicación de Internet donde exista.
        iii. Información técnica necesaria para reproducir, incluidas capturas de pantalla o texto de cualquier código de prueba de concepto.
    c. Una declaración que permita a los investigadores enviar informes anónimos.
    d. Una solicitud de información de contacto del remitente y permiso para hacer un seguimiento de las preguntas técnicas (pero considere si las leyes de privacidad locales y estatales permiten exenciones de la información de contacto personal de las solicitudes de acuerdo con la ley de libertad de información).
5. Una declaración pública de que su organización:
    a. “No recomendará ni iniciará acciones legales” contra nadie por actividades de investigación de seguridad que representen, en opinión de su organización, un esfuerzo de buena fe para seguir esta política.
    b. Que tales actividades se “consideren autorizadas”.
6. Una fecha de emisión.

- **A su discreción, las Políticas de Divulgación de Vulnerabilidades pueden incluir estos elementos:**

1. Una declaraci· n de que su organizaci· n acusar§ recibo de todos los env²os a vuelta de correo electr· nico (donde se proporcione) dentro de un cierto n¼mero de d²as.
    - Siete d²as es est§ndar para una respuesta personal, 24 horas para una respuesta autom§tica.
    - La mayor²a de los programas de divulgaci· n de vulnerabilidades asignan un n¼mero de caso con fines de seguimiento.
2. Si aplica, una declaraci· n de que su organizaci· n se comunicar§ con el remitente si se necesita su ayuda para reproducir o solucionar los problemas, y si han proporcionado un m®todo de comunicaci· n de devoluci· n.
3. Una declaraci· n de que su organizaci· n agradecer§ al remitente cuando crea que el problema se ha resuelto.
4. Una solicitud de que los remitentes no proporcionen un volumen alto espec²fico de informes por d²a/semana (es decir, m§s de 25) o informes automatizados, tales como la salida de escaneos.
5. Una declaraci· n de que los env²os pueden compartirse con otras agencias gubernamentales electorales o de ciberseguridad, o con proveedores de productos, con el ¼nico prop· sito de mitigar el riesgo identificado en los sistemas electr· nicos.
6. Una solicitud de que cualquier vulnerabilidad de seguridad del producto no descubierta previamente ("d²as cero") se divulgue al proveedor del producto o a un coordinador externo previamente establecido.

- **Otras aspectos a considerar la estructura de su Política de Divulgación de Vulnerabilidades:**
    - Muchas organizaciones prohíben explícitamente la ingeniería social (como el phishing), que a menudo se emplea en pruebas de penetración comerciales legítimas.
    - Las organizaciones pueden optar por colocar ciertos sistemas confidenciales fuera de alcance.
    - Los investigadores pueden ver información confidencial en el curso de la identificación de vulnerabilidades de seguridad:
        - Muchas políticas establecen que los investigadores no deben modificar ni acceder a datos más allá de lo necesario para demostrar la prueba de concepto.
        - La mayoría de las políticas prohíben explícitamente compartir dichos datos con terceros.

- **Debido a que muchos investigadores de seguridad son profesionales que buscan reconocimiento, los acuerdos de confidencialidad que les impiden hablar sobre su trabajo después de que el problema ha sido solucionado pueden disuadirlos de prestar su ayuda a su organización.**

- **Las organizaciones pueden considerar pagar una "recompensa por errores" (es decir, una recompensa por vulnerabilidades informadas y validadas).**

    a. Estos programas alientan a un mayor número de investigadores a iniciar las pruebas.

    b. Los programas de recompensas por errores también pueden aumentar los recursos (en términos de tiempo del personal y dólares del programa) necesarios para mantener un programa.

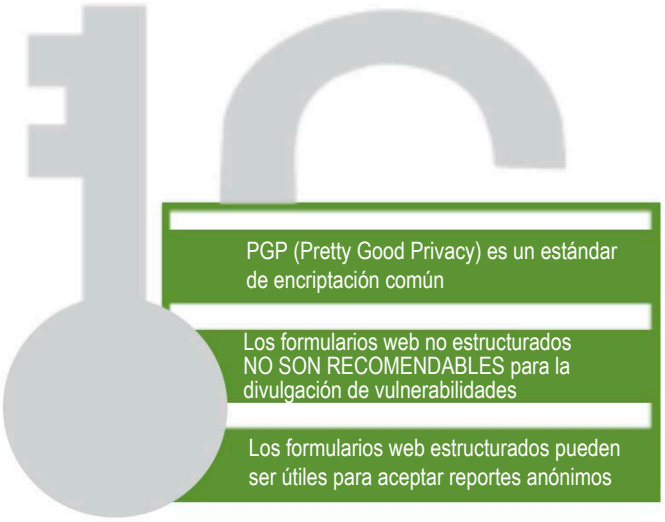
    c. Muchas organizaciones operan inicialmente su programa de divulgación de vulnerabilidades sin ofrecer compensación financiera a los investigadores mientras desarrollan su propia capacidad para solucionar problemas identificados y comunicarse con los investigadores.

PASO 3 Establecer una forma de recibir informes/enviar comunicaciones de seguimiento

- **Antes de publicar una Política de Divulgación de Vulnerabilidades, su entidad debe establecer un método para recibir reportes no solicitados sobre posibles vulnerabilidades de ciberseguridad.**

- **Por lo general, pero no siempre, es una dirección de correo electrónico genérica con el dominio de su organización que múltiples funcionarios pueden acceder (algunas organizaciones usan una página web de registro).**

La dirección de correo electrónico o la página de registro debe ofrecer una clave encriptada pública para proteger el envío de datos, y los funcionarios que acceden a estos mensajes deben tener una clave privada



- **Puede considerar tener direcciones separadas de "Seguridad@" y "Vulnerabilidades@" para asegurarse de que la información sobre incidentes de seguridad en vivo se lean inmediatamente.**

- **Si su organización tiene un dominio .gov, considere actualizar su información de contacto de seguridad en el registrar.gov, asegurándose de que es una dirección de correo electrónico genérica monitoreada regularmente.**

  - Si su organización tiene un dominio .gov, debe registrar su dirección de correo electrónico de contacto de seguridad en dotgov.gov; esto permite que los investigadores de seguridad que identifican problemas relacionados con su dominio se comuniquen con usted.

- **Su entidad también debe establecer direcciones de correo electrónico grupales para la comunicación de seguimiento con investigadores que están separados de las direcciones de correo electrónico de los funcionarios individuales.**

  - Los investigadores de seguridad esperarán que los destinatarios de los informes de vulnerabilidad permanezcan en contacto, y una cuenta compartida permite que las responsabilidades de seguimiento y actualización de estado se distribuyan entre varios funcionarios.

  - Una cuenta compartida también garantiza que las cuentas de correo electrónico de trabajo individuales de los funcionarios estén disponibles para otros asuntos de rutina (las solicitudes de actualizaciones pueden ser frecuentes).

PASO 4 Asignar a alguien para agradecer y comunicarse con los investigadores

- **La coordinación de vulnerabilidades tiene tanto que ver con la comunicación como con las soluciones técnicas.**
- **Los investigadores de seguridad pueden ayudarlo a descubrir puntos débiles en sus sistemas electrónicos y reducir el riesgo en sus operaciones electorales.**
- **Es más probable que los investigadores de seguridad detecten vulnerabilidades en los sistemas de las organizaciones que reconocen sus informes y establecen una expectativa razonable sobre la comunicación bidireccional.**

QUÉ ESPERAN LOS INVESTIGADORES DE USTED

ALGUNA FORMA DE RECONOCIMIENTO (A MENUDO ALGO TAN SIMPLE COMO UN CORREO ELECTRÓNICO DE AGRADECIMIENTO)

EN LA MAYORÍA DE LOS CASOS, QUIEREN SABER QUE USTED RECIBIÓ SU MENSAJE Y SI ESPERA MÁS COMUNICACIÓN

A MENUDO QUIEREN HACER SUGERENCIAS PARA AYUDARLE A SOLUCIONAR EL PROBLEMA (UNA BUENA EXPERIENCIA DE CAPACITACIÓN PARA SU PERSONAL DE IT)

SI ES POSIBLE, DELES CRÉDITO A SU NOMBRE O SEUDÓNIMO EN UN ANUNCIO PÚBLICO PARA SU AVANCE PROFESIONAL (ALGUNOS DESEARÁN PERMANECER ANÓNIMOS)

ALGUNOS INVESTIGADORES DE VULNERABILIDAD BUSCARÁN SU APROBACIÓN PARA PUBLICAR SUS HALLAZGOS (CÓMO SE DESCUBRE Y SE SOLUCIONA EL PROBLEMA) DESPUÉS DE QUE USTED LO SOLUCIONE DE NUEVO, PARA AMPLIAR SUS CREDENCIALES ACADÉMICAS O PROFESIONALES

POR ESTO ES IMPORTANTE DECLARAR OFICIALMENTE EL CASO "CERRADO" EN UN CORREO ELECTRÓNICO

LA MAYORÍA DE LOS INVESTIGADORES QUE PRUEBAN LOS SISTEMAS ELECTORALES NO ESTÁN BUSCANDO DINERO (A MENOS QUE EXISTA UN PROGRAMA DE RECOMPENSAS POR ERRORES)

A LOS INVESTIGADORES ACADÉMICOS A MENUDO SE LES PROHÍBE ACEPTAR COMPENSACIÓN EXTERNA

- **Según una encuesta del 2016, el 57 % de los investigadores esperaba participar en las pruebas de mitigación de las vulnerabilidades identificadas y el 53 % esperaba reconocimiento.[1].**
- **Un 50% de los investigadores también consideraron divulgar públicamente antes de que el problema fuera solucionado debido a la frustración de trabajar con el propietario del sistema, según la misma encuesta.**

1 Departamento de Comercio de EE. UU., Administración Nacional de Telecomunicaciones e Información (NTIA), Informe del Grupo de Adopción y Concientización de Múltiples Partes Interesadas: Vulnerability Disclosure Attitudes & Actions, 2016

PASO 5 Asignar a alguien para examinar y corregir las vulnerabilidades

Un programa de mitigación de vulnerabilidad requiere más que una política de divulgación; requiere wue el persoal tenga tiempo para investigar y solucionar los problemas y para mantener informados a los investigadores (si no están involucrados).

PASOS

1 Admisión y Triaje

- El personal de su organización o un contratista externo revisa los nuevos informes de vulnerabilidad y realiza una evaluación inicial de plausibilidad.
- Si un reporte parece representar un problema de seguridad plausible, el personal de clasificación asigna un "caso" para alguien responsable de administrar el elemento o sistema afectado.
- Su personal envía un mensaje de reconocimiento a aquellos investigadores que brinden su información de contacto, por lo general, utilizando lenguaje estándar.
  - Si un informe no parece útil, la respuesta inicial agradece al investigador por su ayuda y "cierra el caso", con una declaración de "No se tomarán medidas adicionales".
  - Si un reporte amerita una acción adicional, la respuesta inicial debe indicar que usted podrá hacer más preguntas de seguimiento y que les notificará cuando se haya solucionado.

2 Discusión y Arreglo

- El personal de IT de su organización da prioridad a las vulnerabilidades que necesitan parches, reconfiguración u otra acción en el orden de riesgo que representan para su misión.
- A medida que su personal de IT intente solucionar el problema reportado, es posible que deban pedir ayuda al investigador para reproducir el problema o comprobar si está solucionado.

3 Cieere de caso

- Cuando su organización haya terminado de trabajar en un problema, cierre el "caso" y envíe un mensaje de agradecimiento al investigador (si es posible).
- Algunas organizaciones envían una calcomanía para el parachoques, un llavero u otro obsequio simbólico a los investigadores que hayan sido particularmente útiles en el reporte o la solución de problemas.
- Los proveedores a menudo publican un boletín de seguridad pública que acredita a los investigadores que buscan reconocimiento.
- **IMPORTANTE:** Los investigadores tomarán este mensaje final como aprobación para publicar una descripción de sus hallazgos, sus métodos de prueba y, en ocasiones, sus correos electrónicos para una audiencia pública, a menos que ustedes hayan acordado lo contrario.

PASO 6 Considerar compartir información con otras partes afectadas

- **Muchos administradores electorales usan combinaciones similares de hardware y software, y todos están amenazados por los mismos actores maliciosos que buscan socavar la confianza pública en el proceso de votación.**
    - Si cree que un problema reportado en sus sistemas podría afectar a otros administradores electorales y si sus obligaciones legales lo permiten, debería considerar compartir un resumen de vulnerabilidad y mitigación con otras entidades.
    - Si un investigador le informa una vulnerabilidad que se relaciona con un defecto de diseño en el software o hardware de un producto y cree que es "novedoso" (es decir, desconocido para el fabricante), debe considerar compartir la información con el fabricante o un coordinador de terceros como la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA).
    - La junta electoral de su estado, el Centro de Análisis e Intercambio de Información de Infraestructura Electoral (EI-ISAC), CISA y la Comisión de Asistencia Electoral (EAC) pueden ayudar.
- **La divulgación pública de las cosas que ha solucionado contribuye a que los ciudadanos sientan que usted tiene el control en manejo del riesgo de seguridad cibernética, y ayuda a manejar el mensaje.**

ANEXO I. Diferencia entre "vulnerabilidades de día cero", vulnerabilidades de seguridad estándar y errores

- **Prácticamente todas las vulnerabilidades reveladas a los administradores electorales son vulnerabilidades de seguridad estándar que pueden ser solucionadas sin un proceso de coordinación complejo.**
- **Corrección de vulnerabilidades de seguridad = PRIMEROS AUXILIOS.**
- **Corrección de vulnerabilidades del día cero = DESARROLLO DE UNA CURA PARA UNA ENFERMEDAD RECIENTEMENTE DESCUBIERTA (Llamar a un especialista).**
- **Esta analogía no funciona cuando los administradores electorales tienen sistemas patentados o personalizados creados por proveedores que ya no existen, o cuando proveedores de computación en la nube y SaaS están involucrados.**
    - Estos temas están más allá del alcance de este documento, pero requieren de más discusión.

o En orden creciente de seriedad:

o *Bugs* son errores en el diseño o funcionamiento de un problema de software o hardware que hacen que se comporte de manera indeseada, pero que no necesariamente afectan la seguridad.

o Vulnerabilidades de seguridad son atributos comunes de un hardware, software, proceso o procedimiento que podrían permitir o facilitar el daño de un control de seguridad[2].

- Las vulnerabilidades de seguridad permiten que se creen efectos negativos en la confidencialidad, integridad o disponibilidad de los sistemas o datos en esos sistemas.
- Las vulnerabilidades de seguridad pueden causarse por a una configuración incorrecta del usuario, un error del fabricante o problemas imprevistos en la interacción de los elementos.
    - Las vulnerabilidades de seguridad son problemas comunes y ampliamente conocidos que pueden existir en una red.
    - Cuando se identifican, las vulnerabilidades de seguridad se pueden corregir sin demorar la publicación.

o Vulnerabilidades del día cero son fallas en el código de los componentes de software y hardware que son comunes a todas las copias de una versión en particular y son desconocidas para el proveedor del componente.

- Debido a que estas son vulnerabilidades latentes/ocultas que pueden utilizarse para dañar prácticamente a todos los usuarios de un producto vulnerable, es fundamental que el fabricante del producto tenga la oportunidad de identificar medidas de mitigación antes de que el problema sea divulgado públicamente.
- Las vulnerabilidades del día cero pueden afectar un componente del sistema integrado en cientos o miles de productos diferentes, y la publicación retrasada avanzar en la coordinación.
- Una vez que la mitigación/parche está disponible para una vulnerabilidad del día cero, la divulgación pública debe difundirse a lo largo y ancho para evitar que los usuarios que aún no la han solucionado sean explotados.

[2] Vea 6 U.S.C. 1501(17)

ANEXO II. Antecedentes Recursos de consulta

1. **Para una perspectiva de código abierto: [Disclose.io]** **USA Elections Core Terms**

2. **Departamento de Justicia de los Estados Unidos:** **Framework for a Vulnerability Disclosure Program for Online Systems** (Julio de 2017)

    - Una guía práctica para crear un programa de divulgación de vulnerabilidades que fomentará una conducta de apoyo por parte de los investigadores de seguridad y manejará los problemas según la Ley para el Abuso y el Fraude informático.

3. **Universidad Carnegie Mellon: Instituto de Ingeniería de Software:** **CERT Guide to Coordinated Vulnerability Disclosure** (Septiembre de 2019)

    - Una guía de solución de problemas y consejos para la comunicación con los investigadores de seguridad y la coordinación de informes de vulnerabilidad.

4. **Election Infrastructure Information Sharing and Analysis Center** **(EI-ISAC)**

    - Una organización de miembros de administradores electorales que comparte información sobre amenazas y gestión de riesgos cibernéticos.

5. **CISA/Oficina de Administración y Presupuesto:** **Draft Binding Operational Directive 20-01, "Develop and Publish A Vulnerability Disclosure Policy"** (Noviembre de 2019 BORRADOR)

    - Un borrador de Directivas Operacionales que vinculante Agencias del poder ejecutivo del gobierno de los EE. UU. que les exige desarrollar un programa para recibir y solucionar problemas de vulnerabilidad identificados por miembros del público.

6. **Gobierno de los Países Bajos - Ministerio de Seguridad Nacional:** **Responsible Disclosure Policy For Central Government Agencies**

    - Un ejemplo de un programa centralizado de divulgación de vulnerabilidades de largo plazo y exitoso para múltiples entidades dentro de un gobierno.

ANEXO III. Política MODEL de divulgación de vulnerabilidades

- **El modelo de política de divulgación de vulnerabilidades a continuación fue concebido para una agencia federal con muchos dominios en la red, rangos de IP y múltiples niveles de operadores de red.**

- **Si bien representa un enfoque de mejores prácticas, un primer intento exitoso para una entidad más pequeña con una arquitectura cibernética menos compleja puede ser mucho menos detallado.**

Plantilla de política de divulgación de vulnerabilidades

Esta plantilla está destinada a ayudar a su entidad en la creación de una política de divulgación de vulnerabilidades (VDP) basada en el estándar de la agencia federal en Draft Binding Operational Directive (BOD) 20-01

- *Las instrucciones sobre cómo usar la plantilla se proporcionan a lo largo del documento en azul y texto en cursiva y debe borrarse de su política publicada.*
- *Le recomendamos que modifique la plantilla para adaptarla a sus necesidades. Le sugerimos encarecidamente que utilice el lenguaje de la plantilla para la sección de Autorización.*
- *CISA recomienda que revise la guía de implementación que existe como apoyo de la directiva que aplica a las políticas de las agencias federales, en particular "Consider prior art".*
- *Su política debe publicarse como una página web y debe especificar su ubicación en la página de seguridad.txt de su agencia*

Las fuentes principales para esta plantilla fueron Technology Transformation Services' VDP de la Administración de Servicios Generales,el VDP del Departamento de Defensa, y una plantilla VDP de un grupo de trabajo de 2016 de la Administración Nacional de Telecomunicaciones e Información.
Ha sido escrito de acuerdo con el Framework for a Vulnerability Disclosure Program for Online Systems del Departamento de Justicia.

MUESTRA

Política de divulgación de vulnerabilidades

Nombre de la entidad

Día / Mes / Año

Introducción

Una sección inicial que proporciona información general sobre su organización y su VDP. Debe adoptar un tono comprometido, interesado y receptivo.

Nombre de la entidad se compromete a garantizar la integridad de nuestras elecciones asegurándose de que se lleven a cabo sin interferencias maliciosas ni divulgación injustificada de información protegida. Esta política tiene como objetivo brindar a los investigadores de seguridad pautas claras para realizar actividades de descubrimiento de vulnerabilidades y transmitir nuestras preferencias sobre cómo enviarnos las vulnerabilidades descubiertas.

Esta política describe **qué sistemas y tipos de investigación** están protegidos por esta política,**cómo enviarnos** reportes de vulnerabilidad, y **cuánto tiempo** le pedimos a los investigadores de seguridad que esperen antes de revelar públicamente las vulnerabilidades.

Queremos que los investigadores de seguridad se sientan cómodos informando las vulnerabilidades que han descubierto, tal como se establece en esta política, para que podamos corregirlas y mantener a nuestros usuarios seguros. Hemos desarrollado esta política para reflejar nuestros valores y mantener nuestro sentido de responsabilidad hacia los investigadores de seguridad que comparten su experiencia con nosotros de buena fe.

Pautas

De acuerdo con esta política, la investigación significa actividades en las que usted:

- Nos notifica lo antes posible después de descubrir un problema de seguridad real o potencial.
- Hace todo lo posible para evitar las violaciones de privacidad, la degradación de la experiencia del usuario, la interrupción de los sistemas de producción, y la destrucción o manipulación de datos.
- Solo usa exploits en la medida que sean necesarios para confirmar la presencia de una vulnerabilidad. No utilice un exploit para comprometer o filtrar datos, establecer el acceso a la línea de comandos y/o de persistencia, ni utilice el exploit para acceder a otros sistemas.
- Darnos una cantidad de tiempo razonable para resolver el problema antes de divulgarlo públicamente.
- No enviarnos un volumen significativo de reportes de baja calidad.

Una vez que haya establecido que existe una vulnerabilidad o encuentre datos confidenciales (incluida información de identificación personal, información financiera o información de propiedad o secretos comerciales de cualquier parte), debe detener su prueba, notificarnos de inmediato y no divulgar estos datos a nadie más.

Autorización

Esta sección refleja su compromiso de no iniciar acciones legales contra el público en general por actividades de investigación de seguridad que representen un esfuerzo de buena fe para seguir esta política.

*CISA le **sugiere** mantener este lenguaje como está, ya que ha sido diseñado para que sea lo más amable posible para los investigadores, y evitar "jerga legal" u otro lenguaje innecesariamente intimidante.*

Si hace un esfuerzo honesto para cumplir con esta política durante su investigación de seguridad, consideraremos que su investigación está autorizada y Nombre de agencia no recomendará ni iniciará acciones legales relacionadas con su investigación. En caso de que un tercero inicie una acción legal contra usted por actividades realizadas de acuerdo con esta política, le daremos a conocer esta autorización.

Alcance

Esta sección define qué sistemas o servicios accesibles por Internet están dentro del alcance de su política. Su VDP publicado debe ofrecer a los investigadores un sistema o servicio para hacer pruebas, y también debe describir los tipos de pruebas están permitidas (o específicamente no autorizadas).

*Alternativamente, en lugar de dar una **lista de pruebas permitidas** que enumere los sistemas o servicios que están dentro del alcance, puede optar por utilizar una **lista de bloqueos** para describir cuáles están fuera de alcance.*

Asegúrese de tener la autoridad para aprobar las pruebas de seguridad en los sistemas o servicios que se vayan a incluir. Específicamente, si contrata proveedores (por ejemplo, tiene un proveedor de servicios administrados o usa software como servicio), confirme si dicho tercero ha autorizado explícitamente dichas pruebas, dentro del contrato de su agencia con el proveedor o una política disponible públicamente por proveedor. De lo contrario, debe coordinar con el proveedor para obtener la autorización. Si no es posible obtener autorización del proveedor, deberá excluir esos sistemas o servicios de su protocolo.

Nota:

- Después de la publicación de su política, los sistemas o servicios accesibles por Internet recién creados deben estar implícitamente incluídos en el alcance (por ejemplo, indicando un comodín [*] en el alcance de un *dominio) o explícitamente al actualizar la política con el fin de contar con dichos sistemas.*

- *Como se mencionó anteriormente, si no puede obtener autorización para sistemas o servicios específicos proporcionados por terceros, estos deben ser excluidos de las pruebas en su VDP. Sin embargo, debe tratar de incluir dentro del alcance de su política a todos los sistemas o servicios accesibles por Internet utilizados por su agencia, ya que pueden representar un riesgo para su agencia, incluso si están alojados o son proporcionados por terceros.*

Esta política se aplica a los siguientes sistemas y servicios:

- *.agency-brand.gov
- agency-form.gov
- agency-service.gov, and the following hostnames:
  - alpaca.agency-service.gov
  - buffalo.agency-service.gov
  - cassowary.agency-service.gov
  - dormouse.agency-service.gov
  - Cualquier otro subdominio de agency-service.gov todas las aplicaciones de los clientes están excluidos de esta política(*.app.agency-service.gov está específicamente excluido, excepto por *.service-proxy.app.agency-service.gov.)
- código fuente en https://github.com/agency-example/repo

Cualquier servicio que no haya sido mencionado expresamente en la lista anterior, tal como cualquier servicio conectado (es decir, servicios en la nube o de software como servicio), está excluido del alcance y no están autorizados para pruebas. Además, las vulnerabilidades encontradas en sistemas de nuestros proveedores que no tienen el NOMBRE DE LA ENTIDAD quedan fuera del alcance de esta política y deben ser reportados directamente al proveedor de acuerdo con su política de divulgación (si así corresponde). Si no está seguro que un sistema o endpoint está dentro del alcance o no, contáctenos en changeme@entity.gov antes de comenzar su investigación o en el contacto de seguridad para el nombre de dominio del sistema que figura en el .gov WHOIS

Aunque desarrollamos y mantenemos otros sistemas o servicios accesibles por Internet, le pedimos que la investigación y la pruebas activas solo se lleven a cabo en los sistemas y servicios cubiertos por el alcance de este documento. Si hay un sistema en particular que no está dentro del alcance y usted considera que debe ser probado, comuníquese con nosotros para discutirlo primero. Es posible que ampliemos el alcance de esta política con el tiempo.

Tipos de pruebas

Los siguientes tipos de pruebas no están autorizados:

- Pruebas de denegación de servicio de red (DoS o DDoS) u otras pruebas que impidan el acceso o perjudiquen un sistema o datos.
- Pruebas físicas (por ejemplo, acceso a la oficina, puertas abiertas, seguimiento), ingeniería social (por ejemplo, phishing, vishing) o cualquier otra prueba de vulnerabilidad no técnica.

Reporte de una vulnerabilidad

Esta sección describe los mecanismos y procesos de comunicación para enviar vulnerabilidades. Debe incluir instrucciones sobre dónde deben enviarse los informes (p. ej., un formulario web, una dirección de correo electrónico), una solicitud de la información que su entidad necesita para encontrar y analizar la vulnerabilidad (p. ej., una descripción de la vulnerabilidad, su ubicación y su impacto potencial; información técnica necesaria para reproducir, cualquier código de prueba de concepto, etc.). Se debe permitir que los reporteros presenten un informe de forma anónima: no debe solicitar el envío de información de identificación personal, aunque puede solicitar que la persona que da el reporte brinde voluntariamente información de contacto.

Este también es un buen lugar para comprometer a su entidad a ser lo más transparente posible sobre los pasos que está tomando durante el proceso de remediación, así como establecer expectativas sobre cuándo el informante puede anticipar el reconocimiento de su informe.

La información enviada bajo esta política se utilizará solo para mitigar o remediar las vulnerabilidades.

Aceptamos informes de vulnerabilidad a través de changeme@agency.gov o en esta forma. Los informes pueden enviarse de forma anónima.

Acusaremos recibo de su informe dentro de los 3 días hábiles. Encuentre nuestra clave de encriptación PGP para correos electrónicos AQUÍ.

Las claves de encriptación PGP son fáciles de usar; las recomendamos como una forma básica de comunicación con los investigadores. Si elige utilizar un formulario web seguro, asegúrese de que tenga una configuración HTTPS segura.

Lo que nos gustaría ver de parte suya

Para ayudarnos a clasificar y dar prioridad a los reportes enviados, recomendamos que sus informes:

- Describa la vulnerabilidad, dónde la descubrió y el impacto potencial si fuese explotada..
- Ofrezca una descripción detallada de los pasos necesarios para reproducir la vulnerabilidad (los scripts de prueba de concepto o las capturas de pantalla son útiles).
- Escrita en inglés, de ser posible.

Por favor mantenga sus informes de vulnerabilidad actualizados enviándonos cualquier información nueva a medida que esté disponible.

Qué puede esperar de parte nuestra

Cuando elige compartir su información de contacto con nosotros, nos comprometemos a coordinar con usted de la manera más abierta y rápida posible.

- Dentro de los siguientes 3 días hábiles, le informaremos haber recibido su reporte.
- En la medida de nuestras posibilidades, le confirmaremos la existencia de la vulnerabilidad y seremos lo más transparente posible sobre los pasos que estamos tomando durante el proceso de remediación, incluidos los problemas o desafíos que pudiesen retrasar la resolución.
- Mantendremos un diálogo abierto para discutir cualquier problema.

Documente el historial de cambios

Versión	Fecha	Descripción
1.0	*Mes, Día, Año*	Primera emisión.