SEGUIMIENTO A HALLAZGOS DE PRUEBAS DE SEGURIDAD

ÍNDICE

1. Introducción

La información reflejada en el presente documento es propiedad exclusiva de Pegasus Control. Cualquier tipo de modificación que se realice sobre el mismo deberá de ser supervisada por personal autorizado. Si en algún momento esta norma no se cumpliese, el contenido del documento sería considerado nulo y carecería de total validez.

La información contenida se divide en una serie de apartados como son:

- Introducción: información explicativa de la distribución de la información contenida en el informe.
- Objetivo: información explicativa del objetivo del documento.
- Confidencialidad: en este apartado se detallan un conjunto de consideraciones relativas a la distribución y confidencialidad del documento.
- Marco de referencia: apartado en donde se enlistan los dispositivos dentro del alcance y su fecha de revisión.
- Metodología: aquí se agrupan un conjunto de recomendaciones de uso para el presente informe.
- Criterio de clasificación del riesgo: explica el criterio de clasificación del riesgo en función del estándar CVSS, (Common Vulnerability Scoring System), y la clasificación del nivel de gravedad.
- Vulnerabilidades detectadas: presenta un listado de vulnerabilidades identificadas en lugares concretos. El concepto de ocurrencia se asocia a un problema de seguridad en una ubicación específica.
- Conclusiones: Resume el estado general de la revisión.

2. Objetivo

El presente documento tiene como finalidad, presentar y describir las bitácoras de remediación o planes para corregir los hallazgos documentados en los informes de resultados de las pruebas de seguridad informática o reportes de análisis de vulnerabilidades así como el plan de seguimiento de las vulnerabilidades.

3. Responsabilidades

Actividades	Responsable
Ejecutar escaneo de vulnerabilidades. Identificar y clasificar los hallazgos para presentarlos.	Sysadmin
Tomar los requerimientos, planificar las actividades y tiempo para contener o resolver los hallazgos encontrados.	Sysadmin
Ejecutar las acciones correctivas dentro del área de aplicativo.	Gerente de producto

Figura 1. Tabla de Responsabilidades

3. Marco de referencia

Definido el protocolo para el seguimiento de hallazgos al escaneo de vulnerabilidades en el documento **PRT-034-TI SEGUIMIENTO A HALLAZGOS EN PRUEBAS DE VULNERABILIDAD** se describen las bitácoras o planes a seguir para remediar los hallazgos evidenciados.

3.1 Alcance

El presente reporte detalla los activos de controles volumétricos que presentaron hallazgos en el escaneo de vulnerabilidades:

Host / IP
servidor repositorio 192.168.1.60
servidor de eventos 192.168.1.61
Computadora de desarrollo 192.168.9.8
Computadora de desarrollo 192.168.9.13
equipo IT 192.168.9.124
equipo IT 192.168.9.125

El análisis de vulnerabilidades se realizó durante la siguiente ventana temporal:

Fecha de Inicio	02-02-2021
Fecha de Fin	02-02-2021

3.2 Hallazgos evidenciados en el escaneo de vulnerabilidades

Criticidad	Baja	Media	Alta
Total	**3**	**18**	**1**

Figura 1: Resumen de vulnerabilidades detectadas

Vulnerabilidad	Activos afectados	Puertos afectados	Riesgo	Recomendación
SSH Server CBC Mode Ciphers Enabled	192.168.1.60 192.168.1.61 192.168.9.124 192.168.9.125	**22**	**BAJA**	• Deshabilitar este modo de encriptación. • Validar que el sitio cuente con certificados.

				• Validar que los certificados estén actualizados. • En caso de filtración, revocar y generar un certificado nuevo.
SSL Certificate Cannot Be Trusted	192.168.9.8 192.168.9.13 192.168.9.124 192.168.9.125	**433**	**MEDIO**	• N/A - Los equipos locales son para pruebas y no es necesario certificado SSL ya que la aplicación no sale a internet. • Validar que el sitio cuente con certificados. • Validar que los certificados estén actualizados. • En caso de filtración, revocar y generar un certificado nuevo.
SSL Self-Signed Certificate	192.168.9.8 192.168.9.13 192.168.9.124 192.168.9.125	**433**	**MEDIO**	• N/A - Los equipos locales son para pruebas y no es necesario certificado SSL ya que la aplicación no sale a internet. • Validar que el sitio cuente con certificados. • Validar que los certificados estén actualizados. • En caso de filtración, revocar y generar un certificado nuevo.
IP Forwarding Enabled	192.168.9.13	**TCP/iP**	**MEDIO**	• Deshabilitar forwarding. • Abrir solo los puertos de comunicación de los protocolos utilizados.

				• Actualizar la versión de los protocolos. • En caso de requerir contraseñas, utilizar el estándar del documento **“POL-004-TI Política de Uso de Contraseñas”.**
HTTP TRACE / TRACK Methods Allowed	192.168.9.8	**80**	**MEDIO**	• N/A - Los equipos locales se utilizan para pruebas de la aplicación. • Abrir solo los puertos de comunicación de los protocolos utilizados. • Actualizar la versión de los protocolos. • En caso de requerir contraseñas, utilizar el estándar del documento **“POL-004-TI Política de Uso de Contraseñas”.**
SSL Medium Strength Cipher Suites Supported (SWEET32)	192.168.9.8 192.168.9.13 192.168.9.125	**433**	**MEDIO**	• Reconfigurar la aplicación para evitar el uso de SSL Medium Strength Cipher Suites Supported (SWEET32). • Validar que el sitio cuente con certificados. • Validar que los certificados estén actualizados. • En caso de filtración, revocar y generar un certificado nuevo.
Apache Multiviews	192.168.9.13	**80**	**MEDIO**	• Aplicación web para pruebas locales.

Arbitrary Directory Listing				Actualizar apache versión mayor a 1.3.22. • Actualizar las versiones de las aplicaciones. • Configurar las aplicaciones para utilizar solo los puertos necesarios. • En caso de requerir contraseñas, utilizar el estándar del documento **POL-004-TI Política de Uso de Contraseñas.**
DNS Server Cache Snooping Remote Information Disclosure	192.168.9.13	**TCP/iP**	**MEDIO**	• Deshabilitar el servidor DNS. • Abrir solo los puertos de comunicación de los protocolos utilizados. • Actualizar la versión de los protocolos. • En caso de requerir contraseñas, utilizar el estándar del documento **“POL-004-TI Política de Uso de Contraseñas”.**
Microsoft Windows SMB Shares Unprivileged Access	192.168.9.13	**TCP/iP**	**ALTA**	• En la manera de lo posible, deshabilitar las carpetas compartidas. • Abrir solo los puertos de comunicación de los protocolos utilizados. • Actualizar la versión de los protocolos

				• En caso de requerir contraseñas, utilizar el estándar del documento **“POL-004-TI Política de Uso de Contraseñas”.**

Figura 2: Desglose de vulnerabilidades detectadas

4. Plan de seguimiento a los hallazgos encontrados

Para el seguimiento de los hallazgos previamente identificados, se levantará un proyecto y reunión en el sistema de trabajo interno **Bitrix**/Peganet para presentar, dar seguimiento y resolver los hallazgos.

Se utiliza como guía lo descrito en el documento **PRT-034-TI SEGUIMIENTO A HALLAZGOS EN PRUEBAS DE VULNERABILIDAD** para determinar los rangos de tiempo en que tienen que ser atendidos los hallazgos.

Color	Descripción
BAJA	Vulnerabilidades que no afectan la operación del aplicativo, son consideradas de baja prioridad y su solución puede ser planificada en alguna versión de actualización y ejecutada en un plazo no mayor a 45 días.
MEDIO	Vulnerabilidades que pueden afectar la operación del aplicativo, son consideradas de media prioridad y su solución debe de ser planificada y ejecutada en un plazo no mayor a 15 días.
ALTA	Vulnerabilidades que afectan totalmente y pueden detener la operación total del aplicativo, la solución debe de ser planificada y ejecutada en un plazo no mayor a 3 días.

Figura 3. Descripción de colores

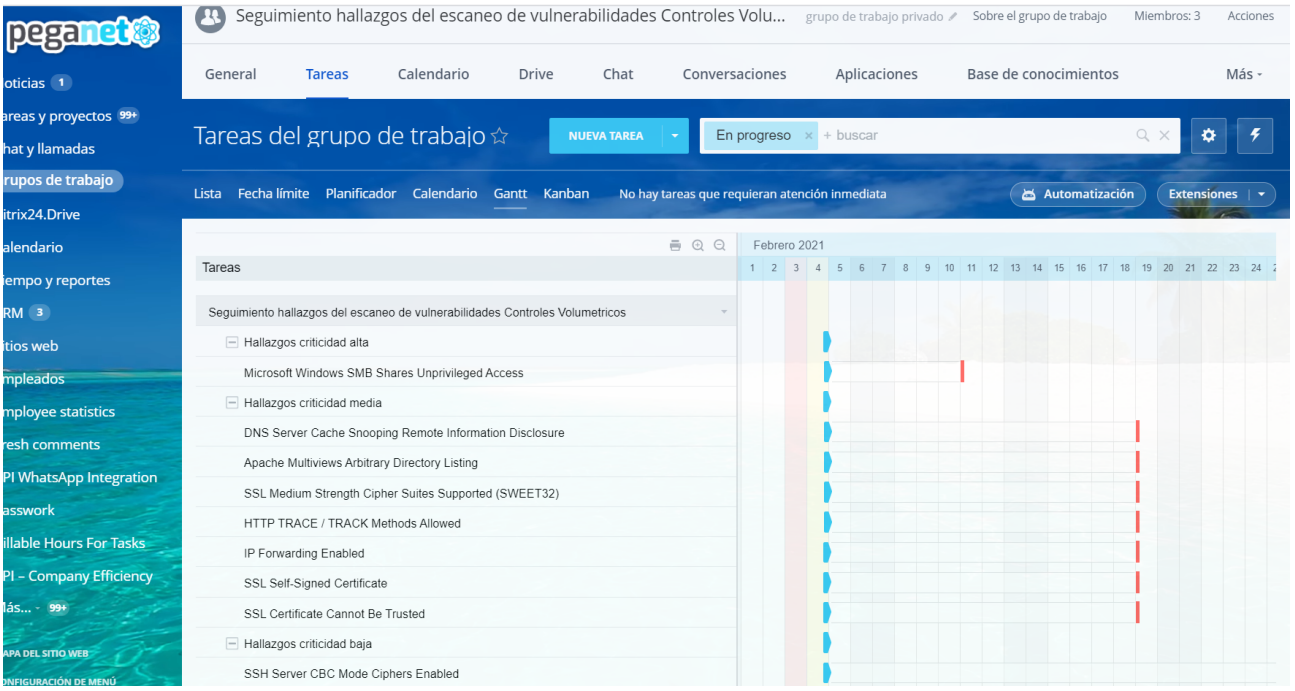

Figura 4. Evidencia de seguimiento a los hallazgos

5. Resultados obtenidos

- De criticidad alta:
  - Microsoft Windows SMB Shares Unprivileged Access
    - Acciones Ejecutadas:
      - Se localiza una carpeta compartida en la Computadora de desarrollo que no tiene contraseña para accesar.
      - Se valida que esa carpeta no tiene razón de ser compartida
      - Se quita el privilegio de carpeta compartida
    - Evidencias:

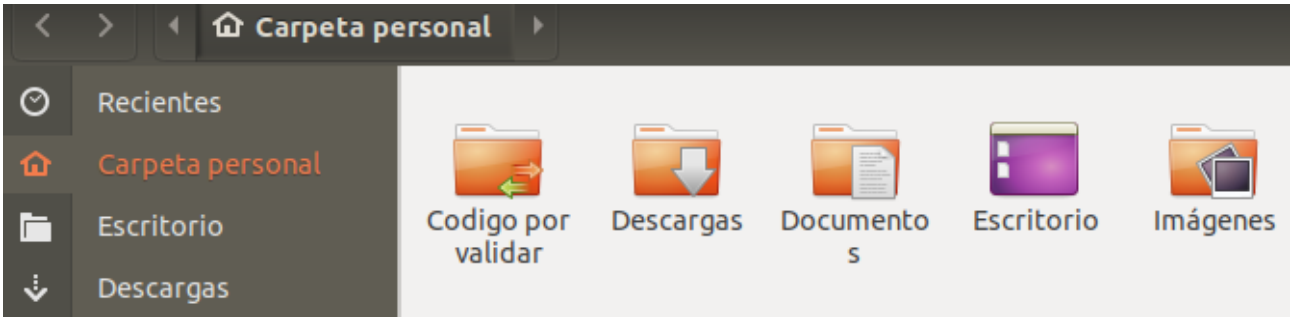

Figura 5 . Se localiza carpeta compartida

Figura 6 . Se deja de compartir la carpeta

- Estado: RESUELTO

6. Historial de Revisiones

Versión	Fecha	Cambios	Elaboró	Revisó	Aprobó
1.0	29/01/2021	Creación de documento	Silvestre Garcia	Rubén Villafuerte	Rubén Villafuerte
1.1	06/12/2022	Revisión de documentación	Omar Aguilar	Rubén Villafuerte	Rubén Villafuerte