FECHA DE EMISIÓN DEL INFORME	**Día:**	04	**Mes:**	07	**Año:**	2023

PROCESO / PROCEDIMIENTO AUDITADO:	Proceso de Apoyo – Gestión de las TIC. OFICINA DE PLANEACIÓN Y SISTEMAS
LÍDER PROCESO AUDITADO:	DR, JORGE CASTRO SALCEDO. Jefe de OFICINA DE PLANEACIÓN Y SISTEMAS (E)
Objetivo de la Auditoría:	Realizar seguimiento al cumplimiento del plan de mejoramiento de la auditoría realizada en la vigencia 2021 y Conocer el nivel de exposición a un ataque externo e Identificar posibles vulnerabilidades de los sistemas de seguridad informática y de la información.
Alcance de la Auditoría:	La presente auditoría inicia con la revisión de las actividades suscritas en el plan de mejoramiento, las evidencias que soportan el avance y/o cumplimiento de las mismas y finaliza con el informe final y sus observaciones y/o recomendaciones y la página web
Criterios de la Auditoría:	Ley 23 de 1982, Sobre derechos de autor, Ley 87 de 1993, Decreto 1078 de 2015, Guías de Seguridad de la Información No.1 al No.21 – Mintic, Norma ISO/IEC 27001, Ley 599 de 2000, Artículo 271. Violación a los derechos patrimoniales de autor y derechos conexos. ISO Guía 73:2002, Anexo 4 - Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas

Reunión de Apertura						**Ejecución de la Auditoría**				**Reunión de Cierre**					
Día	11	**Mes**	04	**Año**	2023	**Desde**	11/04/23 D / M / A	**Hasta**	30/06/23 D / M / A	Día		Mes		Año	

Jefe oficina de Control Interno	Auditor Líder
Dr. ARNULFO RONCANCIO SANABRIA	ALVARO E. OSPINA R. Profesional Universitario Ingeniero de sistemas Abogado

EJECUCIÓN DE LA AUDITORIA

1 -Se revisaron los planes de mejoramiento de auditorias inmediatamente anteriores, cuyos resultados se apreciarán a continuación.
2- Se utilizaron herramientas para realizar pruebas de penetración o vulnerabilidad para la ejecución de ésta auditoria las más populares de código abierto para el escaneo de vulnerabilidades:

1) NMAP
2) OWASP ZAP
3) OPENVAS

Se realizaron exploraciones de vulnerabilidad en servidores, redes, sitios web y aplicaciones seleccionados. Este informe contiene los riesgos potenciales descubiertos de estos análisis. Los riesgos se han clasificado en categorías según el nivel de amenaza y el grado de daño potencial que pueden representar.

PRINCIPALES SITUACIONES DETECTADAS/ RESULTADOS DE LA AUDITORÍA / RECOMENDACIONES/HALLAZGOS:

1. REVISION PLANES DE MEJORMIENTO VIGENCIA ANTERIOR

Con respecto a los planes de mejoramiento de auditorías anteriores, mediante oficio OCCI 1.7-073-2023 se solicita la siguiente información a la Oficina de Planeación y Sistemas:

1. Informar si la entidad cuenta con herramientas para el monitoreo pasivo que permitan rastrear las actividades sospechosa en la red. Indicar las herramientas.

Respuesta: La entidad cuenta con dos herramientas de monitoreo pasivo, la primera de ellas es el entorno web del switch de Core marca Allied Telesis SBx81CFC960 Series, esta herramienta concentra todos los nodos de red ubicados en los centros de cableado de la entidad y permite la búsqueda de los puntos de red que se encuentran aprovisionados en las diferentes áreas de la entidad, estos se logran monitorear de forma lógica y física.

La segunda herramienta es el software mRemoteNG, el cual enlaza los centros de

cableado por direccionamiento IPv4 y es posible monitorear cada switch de la entidad y sus respectivos puntos, este nos permite monitorear de forma lógica y configurar dichas interfaces.

2. Informar si la entidad cuenta con herramientas para el monitoreo activo, que garanticen una vigilancia más exhaustiva de la red, con una cobertura las 24/7. Indicar las herramientas.

Respuesta: La entidad cuenta con dos herramientas para el monitoreo activos 12/7, las primeras de ellas son dos firewalls PALO AL TO PA-3230 en disponibilidad HA, esto significa que al existir la perdida de conexión con el firewall el otro ingresa de forma inmediata a remplazarlo para evitar indisponibilidad de servicios, esta herramienta nos permite filtrar tráfico, y evidenciar en tiempo real consumos altos de internet y ancho de bandas grandes en la red local, de igual forma nos indica en tiempo real ataques he intrusiones de software o IPs malintencionadas que puedan ingresar a nuestra infraestructura.

La segunda herramienta es un software ZABBIX el cual cumple las funciones de monitoreo instantáneo que enlaza por medio de protocolo 1Pv4 los diferentes aplicativos y equipos activos de la entidad, esto nos permite monitorear y evidenciar los diferentes switch puntos de red que posee la entidad.

3. Informar con que herramientas y/o componentes de seguridad perimetral informática cuenta la entidad.

Respuesta: La entidad cuenta con dos firewalls PALO AL TO PA-3230 en alta disponibilidad, para todo el tema seguridad perimetral, igual cuenta con antivirus TRELLIX, para la protección de equipos de cómputo.

4. Informar si la entidad ha implementado métricas para medir políticas de seguridad.

Respuesta: La entidad valida las actividades anómalas de la red y toma acciones inmediatas sobre estas, las cuales son registradas en el GLPI para su seguimiento, pero no se lleva una medición de las métricas identificadas.

OBSERVACIÓN No. 1: Para la auditoria del 2021 se realizó la observación “La entidad no cuenta con métricas de seguridad.” Para el 2022 indicaron que estaban pendiente de realizar, para el 2023, aún no se han implementado. Se observa que persiste el incumplimiento de esta actividad.

2. EXPLORACIÓN DE VULNERABILIDADES

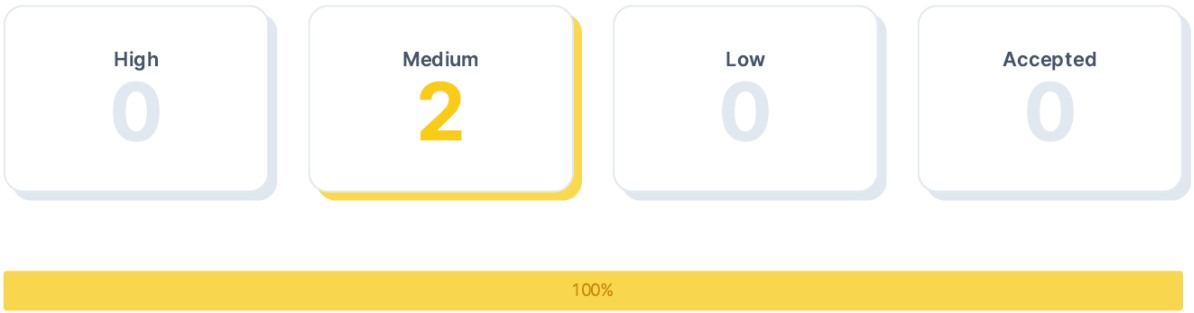
RASTREO CON NMAP

Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos, el cual, permite encontrar qué dispositivos se están ejecutando la su red, descubrir puertos, servicios abiertos y detectar vulnerabilidades.

OBSERVACIÓN NO. 2: El escaneo de puertos TCP NMAP descubre dos (2) puertos TCP abiertos con un escaneo completo de los puertos 0 a 65535.

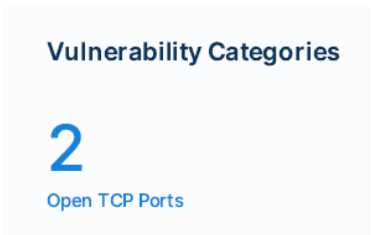
2.1 Riesgos detectados

A continuación se muestra el número total de riesgos encontrados por gravedad. Los riesgos altos son los más graves y deben evaluarse primero. Un riesgo aceptado es aquel que ha sido revisado manualmente y clasificado como aceptable para no corregirlo en este momento, como un falso positivo o una parte intencional de la arquitectura del sistema.



2.2 Alcance del Informe

Este informe incluye los resultados de 1 objetivo que se escaneó. Cada destino es una sola URL, dirección IP o nombre de dominio completo (FQDN).
Categorías de vulnerabilidad:



2.3 Riesgos por objetivo

Esta sección contiene los hallazgos de vulnerabilidad para cada objetivo que se analizó. Priorizando primero los activos más vulnerables.

Target	High	Medium	Low	Accepted
https://www.camara.gov.co/test	0	2	0	0

Open TCP Ports	Threat Level
Open TCP Port: 443	Medium
Open TCP Port: 80	Medium

2.4 Detalles completos de riesgos
Información detallada sobre cada riesgo encontrado por el escaneo.

Puerto TCP abierto: 443

Descripción:
Un puerto abierto puede ser una configuración esperada. Por ejemplo, los servidores web usan el puerto 80 para servir sitios web sobre http y el puerto 443 para servir sitios web sobre https.

Un puerto abierto inesperadamente podría dar acceso no deseado a aplicaciones, datos y redes privadas. Los puertos abiertos también pueden ser peligrosos cuando los servicios esperados están desactualizados y se explotan a través de vulnerabilidades de seguridad.

Puerto TCP abierto: 80

Descripción:
Un puerto abierto puede ser una configuración esperada. Por ejemplo, los servidores web usan el puerto 80 para servir sitios web sobre http y el puerto 443 para servir sitios web sobre https.

Un puerto abierto inesperadamente podría dar acceso no deseado a aplicaciones, datos y redes privadas. Los puertos abiertos también pueden ser peligrosos cuando los servicios esperados están desactualizados y se explotan a través de vulnerabilidades de seguridad.

RASTREO CON OWAS ZAP

Escáner de seguridad de código abierto que permite realizar pruebas de penetración.

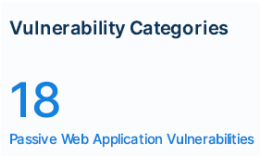
Resumen
Se realizaron exploraciones de vulnerabilidad en servidores, redes, sitios web y aplicaciones seleccionados. Este informe contiene los riesgos potenciales descubiertos de estos análisis. Los riesgos se han clasificado en categorías según el nivel de amenaza y el grado de daño potencial que pueden representar.

OBSERVACIÓN NO. 3: El escaneo de aplicaciones web pasivas OWASP ZAP rastrea las páginas de una aplicación web. Inspeccionó la páginas web, así como las solicitudes y respuestas enviadas entre el servidor. El escaneo pasivo encontró (18) vulnerabilidades como configuraciones incorrectas entre dominios, cookies inseguras, dependencias js vulnerables y más.

3.1. Riesgos Detectados

3.2 Alcance del Informe

Este informe incluye los resultados de 1 objetivo que se escaneó. Cada destino es una sola URL, dirección IP o nombre de dominio completo (FQDN).



(18) Vulnerabilidades de aplicaciones web pasivas o estáticas.

3.3. Riesgos por objetivo

Esta sección contiene los hallazgos de vulnerabilidad para cada objetivo que se analizó. Priorizando primero los activos más vulnerables.

3.4 Resumen de objetivos

El número total de riesgos encontrados para cada objetivo, por gravedad.

Target	High	Medium	Low	Accepted
https://www.camara.gov.co/test	0	9	9	0

3.5 Detalle de los Riesgos encontrados
De Nivel Medio

Ausencia de tokens anti-CSRF (Cross Site Request Forgery).

Descripción

No se encontraron tokens Anti-CSRF en un formulario de envío HTML.

Una falsificación de solicitud entre sitios es un ataque que implica obligar a una víctima a enviar una solicitud HTTP a un destino objetivo sin su conocimiento o intención para realizar una acción como víctima. La causa subyacente es la funcionalidad de la aplicación que usa acciones predecibles de URL/formulario de manera repetible. La naturaleza del ataque es que CSRF explota la confianza que un sitio web tiene para un usuario. Por el contrario, el cross-site scripting (XSS) explota la confianza que un usuario tiene en un sitio web. Al igual que XSS, los ataques CSRF no son necesariamente entre sitios, pero pueden serlo. La falsificación de solicitudes entre sitios también se conoce como CSRF, XSRF, ataque con un solo clic, secuestro de sesión o cabalgamiento de sesión.

Los ataques CSRF son efectivos en una serie de situaciones, que incluyen:

* La víctima tiene una sesión activa en el sitio de destino.
* La víctima se autentica mediante autenticación HTTP en el sitio de destino.
* La víctima está en la misma red local que el sitio de destino.

CSRF se ha utilizado principalmente para realizar una acción contra un sitio de destino utilizando los privilegios de la víctima, pero se han descubierto técnicas recientes para divulgar información al obtener acceso a la respuesta. El riesgo de divulgación de información aumenta drásticamente cuando el sitio de destino es vulnerable a XSS, porque XSS se puede usar como una plataforma para CSRF, lo que permite que el ataque opere dentro de los límites de la política del mismo origen.

Solución:

- ✓ Utilice una biblioteca o un framework que no permitan esta debilidad o proporcione construcciones que hagan que esta debilidad sea más fácil de evitar, ya SEA utilizando paquetes anti-CSRF
- ✓ Asegúrese de que su aplicación esté libre de problemas de secuencias de comandos entre sitios, ya que la mayoría de las defensas CSRF se pueden eludir mediante el uso de secuencias de comandos controladas por atacantes.
- ✓ Genere un nonce (number used only once = NÚMERO USADO SOLAMENTE UNA VEZ) único para cada formulario, coloque el nonce en el formulario y verifique el nonce al recibir el formulario. Asegúrese de que el nonce no sea predecible (CWE-330). Tenga en cuenta que esto se puede anulado usando XSS (código malicioso).

- ✓ Identifique operaciones especialmente peligrosas. Cuando el usuario realiza una operación peligrosa, envíe una solicitud de confirmación por separado para asegurarse de que el usuario tenía la intención de realizar esa operación. Tenga en cuenta que esto se puede anular usando XSS.
- ✓ Utilice el control de gestión de sesiones ESAPI.
- ✓ Este control incluye un componente para CSRF.
- ✓ No utilice el método GET para ninguna solicitud que desencadene un cambio de estado.
- ✓ Verifique el encabezado "HTTP Referer" para ver si la solicitud se originó en una página esperada. Esto podría romper la funcionalidad legítima, porque los usuarios o proxis pueden haber deshabilitado el envío del Refer por razones de privacidad.

Configuración incorrecta entre dominios.

Descripción:

Debido a una posible configuración incorrecta de uso compartido del recursos de origen cruzado (CORS) en el servidor web, se puede producir que se carguen datos de servidores ajenos al acceder a la página web, como contenido malicioso, sin que el usuario lo supiese.

Esta vulnerabilidad se encontró en las siguientes direcciones:

URL	https://connect.facebook.net/es_LA/sdk.js https://connect.facebook.net/es_LA/sdk.js?hash=5cab11b1c6b4d83d142bfd2bb1f3e156 https://platform.twitter.com/widgets.js https://sgdea.camara.gov.co/ControlPQR/CiudadanoPQR/Paginas/Login.aspx
Method	GET
Evidence	Access-Control-Allow-Origin: *

Solución:

- ✓ Asegúrese de que los datos confidenciales no estén disponibles de manera no autenticada (usando la lista blanca de direcciones IP, por ejemplo).
- ✓ Configure el encabezado HTTP "Access-Control-Allow-Origin" en un conjunto de dominios más restrictivo, o elimine todos los encabezados CORS por completo, para permitir que el navegador web aplique la Política del mismo origen (SOP) de una manera más restrictiva.

Direcciones IP potenciales encontradas en Viewstate (Mecanismo usado para almacenar una solicitud específica del usuario y los datos de respuesta entre las peticiones de la página**).**

Descripción:

La vulnerabilidad "Direcciones IP potenciales encontradas en el estado de vista o viewstate" ocurre cuando los datos confidenciales, como las direcciones IP, se almacenan en el estado

de vista de una aplicación web. Si un atacante obtiene acceso a esta información, puede usarlo para lanzar ataques contra el sistema u otros objetivos.

Esta vulnerabilidad se encontró en el siguiente campo del Viewstate:

URL	https://sgdea.camara.gov.co/ControlPQR/CiudadanoPQR/Paginas/Login.aspx
Method	GET

Solución:

- ✓ Verifique que la información proporcionada no sea confidencial.

Falta el encabezado Anti-clickjacking (clicljackin es un ataque donde el usuario cree que esta interactuando con una aplicación y en realidad lo está haciendo sobre un frame superpuesto creado por el atacante)

Descripción:

La respuesta no incluye Content-Security-Policy (CSP)con la directiva 'frame-ancestors' ni X-Frame-Options para proteger contra los ataques de 'ClickJacking':

Esta vulnerabilidad se encontró en la siguiente dirección:

URL	https://sgdea.camara.gov.co/ControlPQR/CiudadanoPQR/Paginas/Login.aspx
Method	GET
Parameter	X-Frame-Options

Solución:

- ✓ Los navegadores web modernos admiten los encabezados HTTP Content-Security-Policy y X-Frame-Options. Asegúrese de que uno de ellos esté configurado en todas las páginas web devueltas por su sitio/aplicación.
  Si espera que la página esté enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET), querrá usar SAMEORIGIN; de lo contrario, si nunca espera que la página esté enmarcada, debe usar DENY. Alternativamente, considere implementar la directiva "frame-ancestors" de la política de seguridad de contenido.

Biblioteca JS (JavaScript) vulnerable.

Descripción:

La biblioteca identificada jquery-ui, versión 1.10.4 es vulnerable.

Esta vulnerabilidad se encontró en la siguiente dirección:

URL	https://intranet.camara.gov.co/core/assets/vendor/jquery.ui/ui/data-

	min.js?v=1.12.1 https://intranet.camara.gov.co/core/assets/vendor/jquery.ui/ui/disable-selection-min.js?v=1.12.1 https://intranet.camara.gov.co/core/assets/vendor/jquery.ui/ui/escape-selector-min.js?v=1.12.1 https://intranet.camara.gov.co/core/assets/vendor/jquery.ui/ui/focusable-min.js?v=1.12.1 https://intranet.camara.gov.co/core/assets/vendor/jquery.ui/ui/form-min.js?v=1.12.1 https://intranet.camara.gov.co/core/assets/vendor/jquery.ui/ui/ie-min.js?v=1.12.1 https://intranet.camara.gov.co/core/assets/vendor/jquery.ui/ui/jquery-1-7-min.js?v=1.12.1 https://intranet.camara.gov.co/core/assets/vendor/jquery.ui/ui/keycode-min.js?v=1.12.1 https://intranet.camara.gov.co/core/assets/vendor/jquery.ui/ui/labels-min.js?v=1.12.1 https://intranet.camara.gov.co/core/assets/vendor/jquery.ui/ui/plugin-min.js?v=1.12.1 https://intranet.camara.gov.co/core/assets/vendor/jquery.ui/ui/safe-active-element-min.js?v=1.12.1 https://intranet.camara.gov.co/core/assets/vendor/jquery.ui/ui/safe-blur-min.js?v=1.12.1 https://intranet.camara.gov.co/core/assets/vendor/jquery.ui/ui/scroll-parent-min.js?v=1.12.1 …
Method	GET

Solución:

- ✓ Actualice a la última versión de jquery-ui.

CSP: Wildcard Directive o Directiva Comodín (Es una regla de CSP que permite que una aplicación web cargue cualquier origen de contenido, lo que lo hace vulnerable a varios ataques.**), Script-src unsafe-inline, Style-src unsafe-inline (**La unsafe-inline palabra clave anula la mayoría de los beneficios de seguridad que el Content-Security-Policy proporciona**.)**

Descripción:

La política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques. Incluyendo (pero no limitado a) Cross SiteScripting (XSS) y ataques de inyección de datos. Estos ataques se utilizan para todo, desde el robo de datos hasta la desfiguración del sitio o la distribución de malware. CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página; los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes,

imágenes y objetos incrustables como subprogramas Java, ActiveX, archivos de audio y video.

Esta vulnerabilidad se encontró en la siguiente dirección:

URL	https://intranet.camara.gov.co/
Method	GET
Parameter	Content-Security-Policy

Solución:

- ✓ Asegúrese que el servidor web, servidor de aplicaciones, balanceador de carga, etc. esté configurado correctamente para establecer el encabezado de Política de seguridad de contenido (Content-Security-Policy).

Content Security Policy (CSP) Header Not Set – Encabezado de política de seguridad de contenido (CSP) no establecido.

Descripción:

La política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. Estos ataques se utilizan para todo, desde el robo de datos hasta la desfiguración del sitio o la distribución de malware. CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página; los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustables como applets de Java, ActiveX , archivos de audio y video.

Esta vulnerabilidad se encontró en la siguiente dirección:

URL	https://sgdea.camara.gov.co/ControlPQR/CiudadanoPQR/Paginas/Login.aspx https://www.camara.gov.co/ https://www.camara.gov.co/404-page https://www.camara.gov.co/admin/ https://www.camara.gov.co/buscador-legislativo https://www.camara.gov.co/codigo-de-etica-y-buen-gobierno https://www.camara.gov.co/comision https://www.camara.gov.co/comision/comision-acreditacion-documental https://www.camara.gov.co/comision/comision-cuarta-o-presupuesto https://www.camara.gov.co/comision/comision-de-derechos-humanos-y-audiencias …
Method	GET
Parameter	Content-Security-Policy

Solución:

- ✓ Asegúrese que el servidor web, servidor de aplicaciones, balanceador de carga, etc. esté configurado correctamente para establecer el encabezado de Política de seguridad de contenido (Content-Security-Policy).

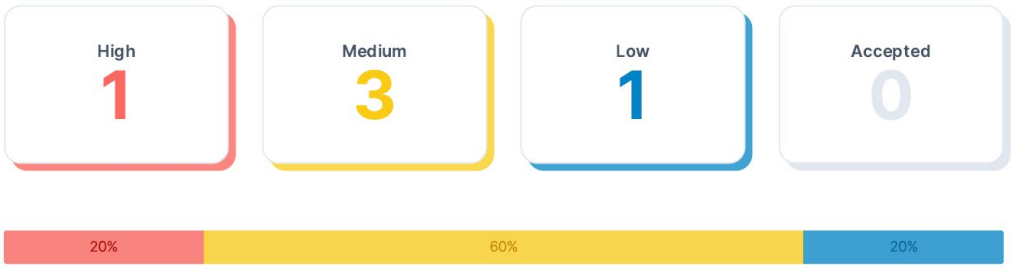
RASTREO CON OPENVAS

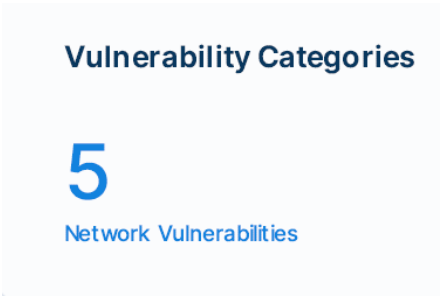
Es un "Open source Vulnerability scanner" que permite encontrar **fallas de seguridad** e información detallada de vulnerabilidades que pueden ser explotadas para poner en peligro la confidencialidad, la disponibilidad y la integridad de los datos almacenados y procesados en nuestros equipos.

El análisis de vulnerabilidades de red de OpenVAS prueba servidores y dispositivos conectados a Internet en busca de más de 50 000 vulnerabilidades. OpenVAS utiliza el Sistema de puntuación de vulnerabilidad común (CVSS) para cuantificar la gravedad de los hallazgos. 0,0 es la gravedad más baja y 10,0 es la más alta.

OBSERVACIÓN No.4: El escaneo con OpenVas detecto (5) riesgos así: (1) de lato riesgo, (3) de nivel medio y (1) de bajo nivel.

Riesgos Detectados





Host	High	Medium	Low	Log	False Positive
23.96.32.104	1	3	1	31	0
Total: 1	1	3	1	31	0

Resultado por Host

Service (Port)	Threat Level
443/tcp	High
443/tcp	Medium
general/tcp	Low
general/CPE-T	Log
443/tcp	Log
80/tcp	Log
general/tcp	Log

Riesgo Alto:

443/tcp - SSL/TLS: Reporte de conjuntos de cifrado vulnerables para HTTPS. Puntaje CVSS (Sistema de puntaje diseñado para proveer un método abierto y estándar que permite estimar el impacto derivado de vulnerabilidades): 7.5

Descripción:

Esta rutina informa todos los conjuntos de cifrado SSL/TLS aceptados por un servicio; donde los vectores de ataque existen solo en los servicios HTTPS. Esta es una debilidad en el cifrado

Estas reglas se aplican para la evaluación de los conjuntos de cifrado vulnerables:

- Cifrado de bloques de 64 bits 3DES vulnerable al ataque SWEET32 (CVE-2016-2183).

Esta puede permitir que un atacante remoto obtenga información confidencial, debido a un error en el cifrado DES/3DES, utilizado como parte del protocolo SSL/TLS. Mediante la captura de grandes cantidades de tráfico cifrado entre el servidor SSL/TLS y el cliente, un atacante remoto capaz de realizar un ataque de tipo "man-in-the-middle" puede aprovechar esta vulnerabilidad para recuperar los datos de texto sin formato y obtener información confidencial.

Resultado de la detección de vulnerabilidad

'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Solución:

La configuración de estos servicios debe cambiarse para que ya no acepte los conjuntos de cifrado enumerados.
Consulte las referencias para obtener más recursos que lo ayuden con esta tarea.

Riesgo Medio:

Métodos de depuración HTTP (TRACE/TRACK) habilitados. Puntaje CVSS: 5.8

Descripción:

TRACK y TRACE son dos métodos que vienen por defecto con Apache HTTPD y que se usan principalmente para análisis, pero estos métodos, usados en WordPress, pueden comprometer la seguridad del sitio ya que hay algunos ataques posibles de Cross Site Tracing (XST) y Cross Site Scripting (XSS) que podrían robar los datos de las cookies y alguna otra información del servidor web, en pocas palabras, un atacante puede usar esta falla para engañar a sus usuarios web legítimos para que le den sus credenciales.

Solución:

- ✓ Deshabilite los métodos TRACE y TRACK en la configuración de su servidor web.
- ✓ Consulte el manual de su servidor web o las referencias para obtener más información.

SSL/TLS: Certificado Expirado – Puntaje CVSS: 5.0

Descripción:

El certificado SSL/TLS del servidor remoto ya ha caducado.

Resultado de la vulnerabilidad detectada:

The certificate of the remote service expired on 2021-02-24 21:01:29.
Certificate details:
fingerprint (SHA-1) | 743227A78143B14CF56526051455BBC9DC225BDE
fingerprint (SHA-256) |
7BBA518E362086382F3552576819A313FB0D35BC0F099F,43551CD851 69715081
issued by | 1.2.840.113549.1.9.1=#726F6F7440535256415A55524543454E
54575757,CN=SRVAZURECENTWWW,OU=SomeOrganizationalUnit,O=SomeOrganization,L=SomeCity
,ST=SomeState, C=--
public key size (bits) | 2048
serial | 7315
signature algorithm | sha256WithRSAEncryption
subject | 1.2.840.113549.1.9.1=#726F6F7440535256415A55524543454E
54575757,CN=SRVAZURECENTWWW,OU=SomeOrganizationalUnit,O=SomeOrganization,L=SomeCity
,ST=SomeState, C=--
subject alternative names (SAN) | None
valid from | 2020-02-25 21:01:29 UTC

valid until | 2021-02-24 21:01:29 UTC

Solución:

- ✓ Reemplace el certificado SSL/TLS por uno nuevo.

SSL/TLS: Detección de protocolo TLSv1.0 y TLSv1.1 en desuso – Puntaje CVSS: 5.0

Descripción:

Fue posible detectar el uso del protocolo obsoleto TLSv1.0 y/o TLSv1.1 en este sistema.

Los protocolos TLSv1.0 y TLSv1.1 contienen fallas criptográficas conocidas como:
- CVE-2011-3389: Explotación del navegador contra SSL/TLS (BEAST).
- CVE-2015-0204: Ataque de factorización en el relleno de claves RSA-EXPORT Oracle en el cifrado heredado degradado (FREAK).

Un atacante podría utilizar las fallas criptográficas conocidas para espiar la conexión entre los clientes y el servicio para obtener acceso a los datos confidenciales transferidos dentro de la conexión segura.

Además, las vulnerabilidades descubiertas recientemente en estos protocolos ya no recibirán actualizaciones de seguridad.

Solución:

- ✓ Se recomienda deshabilitar los protocolos obsoletos TLSv1.0 y/o TLSv1.1 en favor de los protocolos TLSv1.2+. Por favor vea el referencias para más información.

Bajo Riesgo:

TCP (Transmission Control Protocol = Protocolo de Control de Transmisión) timestamps (Permite hacer un cálculo del tiempo que tarda un paquete por la red entre los extremos de la conexión.)

Descripción:

El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.
Se detectó que el host implementa RFC1323/RFC7323.

Las siguientes marcas de tiempo se recuperaron con un retraso de 1 segundo en el medio:
Paquete 1: 3735282707
Paquete 2: 3735283810

Lo anterior facilitaría que un atacante pueda se calcular el tiempo de actividad del host remoto.

Solución: Deshabilitar las marcas de tiempo TCP en Linux, agregue la línea 'net.ipv4.tcp_timestamps

RECOMENDACIONES:

Que se realicen las actividades de mejora dentro de los términos y/o plazos suscritos en el plan mejoramiento.

Que se revisen cada una de las vulnerabilidades detectadas atendiendo a los resultados y posibles soluciones descritas en el presente informe.

CONCLUSIONES DE LA AUDITORÍA

Se observó que de las actividades suscritas en el plan de mejoramiento del 2021, nueve (9) en total, se incumplió con una (1), con un cumplimiento de 90%.

Con respecto al escaneo de seguridad del sitio web de la entidad, se detectó que algunas falencias persisten aunque se han realizado recomendaciones y posibles soluciones, lo que permite inferir, que no han sido efectivas las soluciones aplicadas, o en su defecto no existe un seguimiento y/o monitoreo de las vulnerabilidades detectadas a fin de no permitir que vuelvan a repetir.

Para constancia se firma en Bogotá D.C., a los 05 días del mes de julio del año 2023

APROBACIÓN DEL INFORME DE AUDITORÍA		
Nombre Completo	**Responsabilidad** (cargo)	**Firma**
ARNULFO RONCANCIO SANABRIA	COORDINADOR	
ALVARO ERNESTO OSPINA RAMÍREZ	PROFESIONAL UNIVERSITARIO	
NIDIA CLEMENCIA HERNANDEZ BAQUERO	PROFESIONAL UNIVERSITARIO	
HELIDE RIVERO	CONTRATISTA	
ANGIE PAEZ HERNANDEZ	CONTRATISTA	
DANIELA FERNANDA RIVERO	CONTRATISTA	

CONTROL DE CAMBIOS

Nº VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
1	01/01/2016	Versión inicial del formato
2	28/01/2022	La 2da versión fue aprobada acta 1 Comité Institucional de Gestión y Desempeño llevado a cabo el 28 de enero de 2022 y reformula todo el formato.