

"2022. Año del Quincentenario de Toluca de Lerdo, Capital del Estado de México".

20706007030000L/1118/2022

Toluca de Lerdo, México
a 21 de octubre de 2022

LIC. LINDA ESMERALDA SOMILLED A VENTURA
SUBDIRECTORA DE VINCULACION CIUDADANA
DIRECCION GENERAL DE INNOVACION
P R E S E N T E

Con fundamento en lo dispuesto en el Manual de Organización de la Secretaría de Finanzas, en el apartado 20706007030200L Subdirección de Seguridad Informática, particularmente en lo que respecta a coordinar las pruebas de penetración a los aplicativos de la Red Estatal de Telecomunicaciones, para identificar las vulnerabilidades de la seguridad informática; así como, establecer las medidas para la remediación de vulnerabilidades reportadas.

Por lo anteriormente expuesto, me permito informar que se han detectado vulnerabilidades en el sitio: <http://chat2.edomex.gob.mx>, anexo se envía el escaneo completo con el detalle de todas las vulnerabilidades encontradas.


No omito mencionar que se deben aplicar las recomendaciones que vienen descritas en el documento para anular o minimizar el riesgo presentado. De igual forma, le solicito atentamente se sirva dar remediación y notifique por este mismo medio, cuando se hayan aplicado dichas recomendaciones.

Sin otro particular por el momento, le envío un cordial saludo.

A T E N T A M E N T E


RUBÉN GARCÍA GONZÁLEZ
DIRECTOR DE INFRAESTRUCTURA TECNOLÓGICA
Y COMUNICACIONES

c.c.p. Blanca Azucena Martínez García. Subdirectora de Seguridad Informática
c.c.p. Archivo

	EDOMÉX DECISIONES FIRMES. RESULTADOS FUERTES
SECRETARÍA DE FINANZAS SUBSECRETARÍA DE ADMINISTRACIÓN DIRECCIÓN GENERAL DE INNOVACIÓN SUBDIRECCIÓN DE VINCULACIÓN CIUDADANA	
RECIBIDO POR: <u>Ciem</u>	
HORA <u>12:45</u> FECHA <u>24/10/2022</u>	

SECRETARÍA DE FINANZAS
SUBSECRETARÍA DE ADMINISTRACIÓN
DIRECCIÓN GENERAL DEL SISTEMA ESTATAL DE INFORMÁTICA



Reporte Técnico de Análisis

Código: RTI-171-COMSEG-CONF

Versión: 001

Fecha: 4 OCTUBRE 2022

Número de página 1 de 5

Análisis de seguridad
10.40.130.16 / 201.140.104.6
<http://chat2.edomex.gob.mx/>



Reporte Técnico de Análisis

Código: RTI-171-COMSEG-CONF

Versión: 001

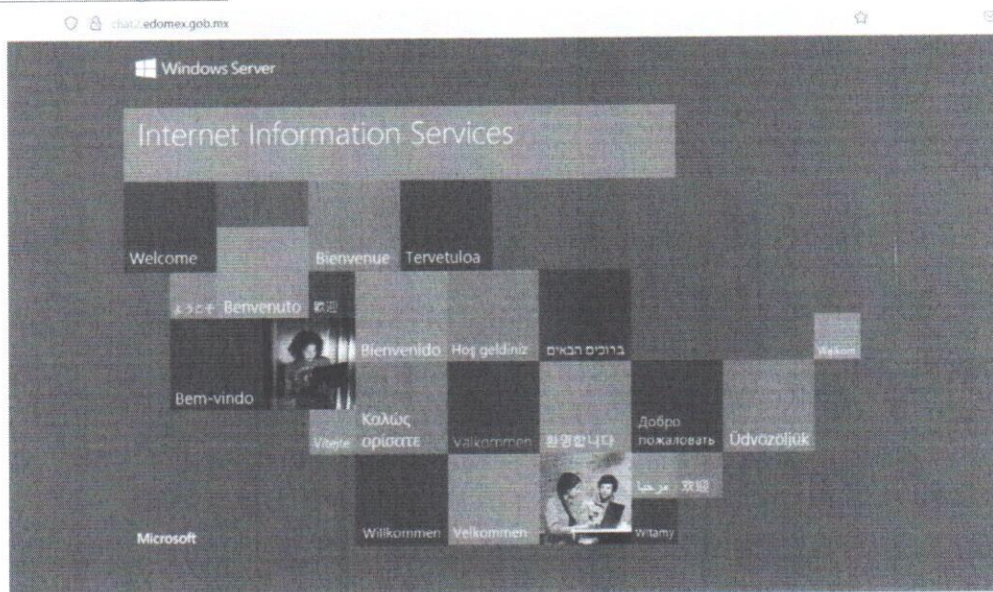
Fecha: 4 OCTUBRE 2022

Número de página 2 de 5

Objetivo

Informar las vulnerabilidades técnicas del sitio web:

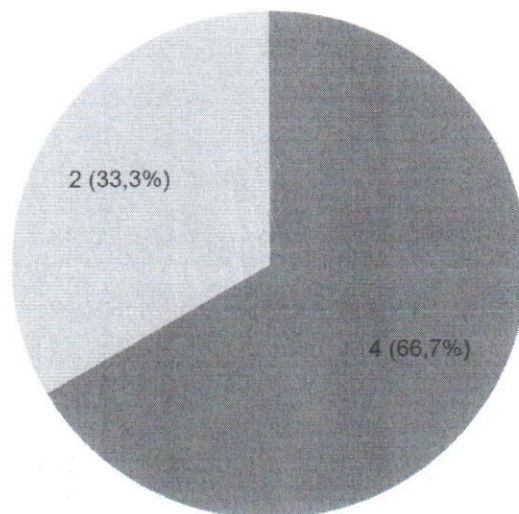
<http://chat2.edomex.gob.mx/>



Resumen de hallazgos

Por Severidad

● Alto ● Medio



Total de hallazgos: 6

1. Severidad Alta. Total: (4)



Reporte Técnico de Análisis

Código: RTI-171-COMSEG-CONF

Versión: 001

Fecha: 4 OCTUBRE 2022

Número de página 3 de 5

a) Content Security Policy (CSP) Header Not Set (1)

Método	Ruta
GET	http://chat2.edomex.gob.mx/

Descripción del riesgo:

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. Se detectó que su aplicación web no implementa la política de seguridad de contenido (CSP) ya que falta el encabezado de CSP en la respuesta.

Recomendación:

Se recomienda implementar la Política de seguridad de contenido (CSP) en su aplicación web. La configuración de la política de seguridad de contenido implica agregar el encabezado HTTP Content-Security-Policy a una página web y darle valores para controlar los recursos que el agente de usuario puede cargar para esa página.

Reference

<https://www.acunetix.com/vulnerabilities/web/content-security-policy-csp-not-implemented/>
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

b) Missing security header: Referrer-Policy (1)

Método	Ruta
GET	http://chat2.edomex.gob.mx/

Descripción del riesgo:

El encabezado HTTP Referrer-Policy controla cuánta información de referencia enviará el navegador con cada solicitud originada en la web actual solicitud.

La configuración de la cookie para la navegación a través del protocolo https no está configurada adecuadamente, por lo que existe un riesgo de que un atacante intercepte la comunicación de texto claro entre el navegador y el servidor.

Recomendación:

El encabezado Referrer-Policy debe configurarse en el lado del servidor para evitar el seguimiento del usuario y la fuga de información inadvertida.

Referencias:

https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

c) Missing security header: X-Frame-Options

Método	Ruta
GET	http://chat2.edomex.gob.mx/

Descripción del riesgo:

Se encontraron encabezados X-Frame-Options (XFO), una respuesta con múltiples entradas de encabezado XFO puede no ser tratada de manera predecible por todos los navegadores.



Reporte Técnico de Análisis

Código: RTI-171-COMSEG-CONF

Versión: 001

Fecha: 4 OCTUBRE 2022

Número de página 4 de 5

Recomendación:

Asegúrese de que solo haya un encabezado X-Frame-Options en la respuesta.

Existen dos posibles directivas para X-Frame-Options:

X-Frame-Options: DENY

X-Frame-Options: SAMEORIGIN

Referencias:

<https://developer.mozilla.org/es/docs/Web/HTTP/Headers/X-Frame-Options>

<https://www.zaproxy.org/docs/alerts/10020-2/>

d) Uso de protocolo http (1)

Método	Ruta
GET	http://chat2.edomex.gob.mx/

Descripción del riesgo:

Un sitio web que funcione bajo el protocolo HTTP no es seguro, podemos poner en riesgo nuestra seguridad y privacidad al realizar navegación de este tipo.

Recomendación:

El uso de HTTPS proporciona a los usuarios la privacidad, seguridad y protección de datos.

Referencias:

<https://www.siteground.es/blog/que-es-https-y-para-que-sirve-guia-completa/>

<https://es.ryte.com/wiki/HTTPS>

2. Severidad Media. (2)

a) Encabezados de seguridad HTTP inexistentes (1)

HTTP Security Header	Header Role	Status
X-Content-Type-Options	Previene phishing o ataques XSS	No habilitado

Descripción del riesgo:

- **X-Content-Type-Options:** Este encabezado evita que se anule el valor del encabezado Content-Type.

Recomendación:

El servidor no devolvió un encabezado 'X-Content-Type-Options' correcto, lo que significa que este sitio web podría estar en riesgo de sufrir un ataque Cross-Site Scripting (XSS)

Referencias:

<https://www.tenable.com/plugins/was/112529>

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options>

b) El servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP ""X-Powered-By"" (1)

Método	Ruta
--------	------



Reporte Técnico de Análisis

Código: RTI-171-COMSEG-CONF

Versión: 001

Fecha: 4 OCTUBRE 2022

Número de página 5 de 5

GET

<http://chat2.edomex.gob.mx/>

Descripción del riesgo:

El servidor de la web/aplicación está divulgando información mediante uno o más encabezados de respuesta HTTP ""X-Powered-By"". El acceso a tal información podría facilitarle a los atacantes la identificación de otros marcos/componentes de los que su aplicación web depende y las vulnerabilidades a las que pueden estar sujetos tales componentes.

Recomendación:

Asegúrese que su servidor web, servidor de aplicación, equilibrador de carga, etc. está configurado para suprimir encabezados ""X-Powered-By".

Referencias:

<http://blogs.msdn.com/b/varunm/Archive/2013/04/23/Remove-Unwanted-http-Response-headers.aspx>

<https://www.analisiswordpress.com/x-powered-by/>

CONCLUSIONES.

Se encontraron 6 vulnerabilidades en el sitio web, de estas vulnerabilidades, 4 son de severidad alta por lo que el riesgo a que la disponibilidad, confidencialidad e integridad del servicio sean comprometidas, es **CRÍTICO**.