INFORME DETALLADO DE ACTIVIDADES EN LOS SIMULACROS OFICIALES

INFORMACIÓN PÚBLICA

Versión	Fecha
1.0	4 de Junio 2021

Contenido

Resumen ejecutivo

A solicitud de la Mtra. Linda Viridiana Calderón Montaño, Consejera Presidenta de la Comisión Temporal del Programa de Resultados Electorales Preliminares, presentamos el siguiente informe detallado de las actividades y pruebas de seguridad informática realizadas durante los **Simulacros Oficiales del Sistema Informático PREP** los días 16, 23 y 30 de mayo 2021.

Los principales aspectos evaluados durante los **Simulacros Oficiales** fueron:

- La disponibilidad del sitio oficial de Presentación de Resultados del Sistema Informático PREP en www.prepsonora.org.mx
- La disponibilidad del sitio oficial del IEEyPC de Sonora en www.ieesonora.org.mx
- La integridad de la información de las Actas PREP procesadas desde la captura y digitalización hasta la publicación de resultados
- La aplicación de la configuración segura sugerida a dispositivos, servidores y redes y la validación de la corrección de vulnerabilidades detectadas en todos los módulos que conforman el **Sistema Informático PREP**

El funcionamiento de los módulos y aplicaciones que conforman el **Sistema Informático PREP** es adecuado, correcto y suficiente, desde el punto de vista de la arquitectura de red, infraestructura y seguridad informática.

En nuestra opinión, los controles técnicos y procesos aplicados razonablemente satisfacen, en su conjunto, el nivel de seguridad necesario para la operación del PREP del 6 al 7 de junio de 2021.

Detalle de actividades

Simulacro 1

Previo al inicio de operación del Sistema Informático PREP se realizó la validación de las correcciones de las vulnerabilidades detectadas por las pruebas de seguridad informática.

Hallazgo / Vulnerabilidad	Fecha de reporte	Estatus
Exposición de información de configuración de aplicaciones mediante directorios con permisos de lectura	23 de abril 2021	**Resuelto**
Exposición de actas digitalizadas y respaldos de la base de datos mediante directorios con permisos de lectura	23 de abril 2021	**Resuelto**
Exposición excesiva de datos del funcionamiento de la aplicación y sus módulos	23 de abril 2021	**Resuelto**
Exposición de información mediante métodos HTTP no soportados	23 de abril 2021	**Resuelto**

Las pruebas realizadas durante el día 16 de mayo de 2021 fueron:

- Validación de apego a pantallas de publicación del PREP y pruebas funcionales del sitio oficial de Presentación de Resultados.
- Pruebas de denegación de servicio
- Pruebas de carga de usuarios concurrentes
- Análisis de vulnerabilidades y configuración segura de los sitios de Presentación de Resultados y del IEEyPC.

Pruebas realizadas

1. El Sistema Informático PREP y sus bases de datos inician la operación con todos los resultados en 0 (cero).
2. El proceso de digitalización, captura, validación, conteo y verificación se revisó en cada una de las etapas y se confirmó que, mediante el uso de firmas criptográficas, se garantiza el flujo correcto del proceso desde el inicio hasta la publicación de actas y resultados.
3. Todos los cálculos aritméticos son correctos.
4. Se detectaron errores en la identificación de casillas en el listado, lo cual impactó en el desempeño del sistema.
5. El simulacro concluyó con el 50% de las actas procesadas.
6. Revisión de acceso no autorizado a la red interna por cable o inalámbrica del Centro de Operaciones del PREP.
7. Revisión de credenciales seguras en dispositivos móviles y aplicaciones.
8. Las pruebas de denegación de servicio realizadas son listadas a continuación:
    a. Ataques distribuidos de 3 Gbps utilizando protocolos UDP, TCP e ICMP dirigido a puertos aleatorios de los servidores www.prepsonora.org.mx, los cuales fueron **mitigados** por los dispositivos de seguridad en la nube.
    b. Ataques distribuidos de 3 Gbps dirigidos a la aplicación *web* de Presentación de Resultados utilizando conexiones lentas, los cuales fueron **mitigados** por los dispositivos de seguridad en la nube.
    c. Simulación de usuarios concurrentes con peticiones válidas al sitio de Presentación de Resultados, lo cual tuvo impacto crítico **afectando por completo la disponibilidad** del sitio oficial de Presentación de Resultados.
    d. Ataques distribuidos de 1 Gbps utilizando protocolos UDP, TCP e ICMP dirigido a puertos aleatorios de los servidores www.ieesonora.org.mx, **afectando por completo la disponibilidad** del sitio oficial del IEEyPC.

Hallazgos principales

El sitio oficial del IEEyPC en www.ieesonora.org.mx y la infraestructura utilizada no cuentan con las capacidades requeridas para mitigar ataques a la disponibilidad.

Durante la simulación de peticiones de usuarios concurrentes a www.prepsonora.org.mx se determinó que al realizar entre [redacted], es posible **afectar parcialmente** la publicación de la información, con tiempos de carga de los datos de hasta 20 segundos.

A partir de los [redacted], los servidores dejan de responder y se **pierde por completo la disponibilidad.** El número total de peticiones realizadas excedió los [redacted] millones de peticiones totales.

Simulacro 2

Durante la operación del Sistema Informático PREP del día 23 de mayo 2021 se realizó la validación de las correcciones de las vulnerabilidades detectadas en el Simulacro 1.

Hallazgo / Vulnerabilidad	Fecha de reporte	Estatus
Configuración del límite de peticiones por usuarios válidos del sitio de Presentación de Resultados	19 de mayo 2021	**Resuelto**
Infraestructura de seguridad insuficiente para mitigar ataques a la disponibilidad del sitio oficial del IEEyPC	19 de mayo 2021	**Resuelto**
Datos incorrectos de identificación de casillas	19 de mayo 2021	**Resuelto**

Las pruebas realizadas durante el día 23 de mayo de 2021 fueron:

- Validación de apego a pantallas de publicación del PREP y pruebas funcionales del sitio oficial de Presentación de Resultados.
- Pruebas de denegación de servicio
- Pruebas de carga de usuarios concurrentes

Pruebas realizadas

1. Confirmación de las correcciones de las bases de datos de casillas en el sitio oficial de Presentación de Resultados.
2. El simulacro concluyó con el 96% de las actas procesadas dentro del rango esperado de tiempo, debido a que el manejo de actas por parte del sistema y los capturistas presentó inconsistencias. Posteriormente se concluyó con la publicación de todas las actas.
3. Las pruebas de denegación de servicio realizadas son listadas a continuación:
    a. Ataques distribuidos de 3 Gbps utilizando protocolos UDP, TCP e ICMP dirigido a puertos aleatorios de los servidores www.prepsonora.org.mx, y a la aplicación utilizando conexiones lentas, los cuales fueron **mitigados** por los dispositivos de seguridad en la nube.
    b. Ataques distribuidos de 3 Gbps utilizando protocolos UDP, TCP e ICMP dirigido a puertos aleatorios de los servidores www.ieesonora.org.mx, y a la aplicación utilizando conexiones lentas, los cuales fueron **mitigados** por los dispositivos de seguridad en la nube.
    c. Simulación de usuarios concurrentes progresivos en intervalos de 500 usuarios [redacted] al sitio de Presentación de Resultados, **sin afectar la disponibilidad y operación.**
    d. Simulación de hasta [redacted] al sitio oficial del IEEyPC sin que esto impacte de manera significativa en la operación.

Hallazgos principales

Existen inconsistencias en el registro y validación de actas PREP que debe ser atendido para garantizar que se digitaliza, procesa y publica el total de registros.

Simulacro 3

Durante el simulacro del día 30 de mayo 2021 se realizó la validación de las correcciones de las vulnerabilidades detectadas en el Simulacro 2.

Hallazgo / Vulnerabilidad	Fecha de reporte	Estatus
Inconsistencias en el registro y validación que evitaron el cierre adecuado de operación	26 de mayo 2021	**Resuelto**

Las pruebas realizadas durante el día 30 de mayo de 2021 fueron:

- Validación del sistema informático del PREP y de sus bases de datos
- Pruebas de denegación de servicio
- Pruebas de carga de usuarios concurrentes

Pruebas realizadas

1. De acuerdo al Procedimiento de validación del sistema informático PREP y sus bases de datos, se ejecutaron los comandos requeridos para obtener las firmas criptográficas de cada uno de los archivos componentes del Sistema Informático PREP en el ambiente de producción para comparar con los archivos previamente revisados dentro del ambiente de auditoría.
2. Ataques distribuidos de 3 Gbps utilizando protocolos UDP, TCP e ICMP dirigido a puertos aleatorios de los servidores www.prepsonora.org.mx, y a la aplicación utilizando conexiones lentas, los cuales fueron **mitigados** por los dispositivos de seguridad en la nube.
3. Ataques distribuidos de 3 Gbps utilizando protocolos UDP, TCP e ICMP dirigido a puertos aleatorios de los servidores www.ieesonora.org.mx, y a la aplicación utilizando conexiones lentas, los cuales fueron **mitigados** por los dispositivos de seguridad en la nube.
4. Simulación de usuarios concurrentes progresivos en intervalos de 500 usuarios [redacted] al sitio de Presentación de Resultados, **sin afectar la disponibilidad y operación.**
5. Simulación con [redacted] al sitio oficial del IEEyPC sin que esto impacte de manera significativa en la operación.

Hallazgos principales

No existen vulnerabilidades explotables de alto impacto.

Conclusión

Con base en los resultados obtenidos de los procesos de pruebas a la disponibilidad, análisis de seguridad y pruebas funcionales al sitio principal del IEEyPC y al sitio de Presentación de Resultados del Sistema Informático PREP podemos concluir que el **riesgo de afectación a la integridad y a la disponibilidad de ambos es** bajo.