pentest
herramienta de diagnóstico eficaz

Informe final de las pruebas funcionales del Sistema Informático PREP

Versión	Fecha
1.0	25 Junio 2018
1.1	30 Junio 2018

Contenido

Introducción 3

Metodologia 4

Criterios utilizados para la auditoría 5

Resumen ejecutivo 6

Resultados 7

Introducción

En el presente documento se muestran los resultados de las pruebas funcionales realizadas al Sistema Informático PREP, se detallan las metodologías utilizadas para las pruebas así como los criterios utilizados.

Se validaron las aplicaciones de PREP Casilla, Prep Casilla Helper y CATD Celular, así como los portales de acceso a las aplicaciones de MCAD, CAPREP y VERIPREP.

Se analizó también el código fuente de las aplicaciones y portales descritos anteriormente mediante un escaneo estático de código.

Metodologia

Las pruebas de penetración realizadas por código verde se apegan a estándares internacionales existentes como Penetration Testing Execution Standard (PTES), Technical Guide to Information Security Testing and Assessment del National Institute of Standards and Technology NIST y Penetration Testing Guidance de Payment Card Industry PCI.

En código verde utilizamos las metodologías, estándares y mejores prácticas para análisis de riesgos y vulnerabilidades propuestas por organizaciones como ISACA (Information Systems Audit and Control Association), EC-Council (International Council of Electronic Commerce Consultants) e (ISC)2 (International Information Systems Security Certification Consortium).

A continuación un resumen general de las etapas del proyecto:

- Interacción previa al inicio de actividades
- Recopilación de información e inteligencia
- Modelo de Amenazas y análisis de vulnerabilidades
- Definición y diseño de vectores de ataque
- Recopilación de evidencias
- Generación de entregables

Adicionalmente se hizo un análisis de código estático sobre las aplicaciones y portales en busca de vulnerabilidades de programación.

Criterios utilizados para la auditoría

El alcance de las pruebas fue delimitado a las aplicaciones:

- PREP Casilla
- Prep Casilla Helper
- CATD Celular

Y a los portales web:

- MCAD
- CAPREP
- VERIPREP

Resumen ejecutivo

Durante los meses de mayo y junio del 2018 se realizaron una serie de pruebas de seguridad con el objetivo de detectar vulnerabilidades en el sistema informático PREP.

De acuerdo al resultado de estas pruebas, código verde emitió una serie de recomendaciones para eliminar vulnerabilidades y mejorar la seguridad de los componentes del sistema informático PREP, las cuales han sido atendidas en su mayoría por el proveedor del sistema informático, de acuerdo a evidencia proporcionada por el mismo.

Resultados

Como resultado de las pruebas, se identificaron hallazgos con impacto en la confidencialidad e integridad del sistema en las siguiente categorías:

- **Permisos y almacenamiento:** se requiere limitar los privilegios de lectura en los servidores que almacenan la información.
- **Transporte de información:** se requiere utilizar conexiones cifradas con certificados para garantizar la integridad de los datos presentados.
- **Configuración segura de dispositivos móviles:** se requiere evaluar la confirmación de los mecanismos de seguridad y acceso remoto del dispositivo y garantizar que la comunicación e información no sea manipulada de manera no autorizada.
- **Actualizaciones y parches de seguridad:** se sugieren actualizaciones del sistema operativo, aplicaciones y componentes de los servidores.
- **Configuración segura de redes:** se requiere implementar controles de red para ocultar y proteger los servidores involucrados en el procesamiento y almacenamiento de información.

Los hallazgos mencionados, fueron evaluados y en su mayoría resueltos por el proveedor del Sistema Informático PREP, presentando evidencia de las correcciones.

En conclusión, podemos afirmar que el riesgo ante posibles ataques a la integridad y confidencialidad en la aplicación Sistema Informático PREP es bajo.

pentest
herramienta de diagnóstico eficaz

Informe final del análisis de vulnerabilidades a la infraestructura tecnológica al Sistema Informático PREP

Versión	Fecha
1.0	25 Junio 2018
1.1	30 Junio 2018

Contenido

Introducción 3

Resultados generales 4

Introducción

En el presente documento se muestran los resultados de las pruebas realizadas a la infraestructura donde se alojan los componentes del sistema información del sistema PREP.

Resultados generales

Durante los meses de mayo y junio del 2018 se estuvieron realizando una serie de pruebas con el objetivo de detectar vulnerabilidades en la infraestructura del sistema informático PREP.

De acuerdo al resultado de estas pruebas, código verde emitió una serie de recomendaciones para eliminar vulnerabilidades y mejorar la seguridad de los componentes de la infraestructura del sistema informático PREP, las cuales han sido atendidas en su mayoría por el proveedor del sistema informático PREP de acuerdo a evidencia proporcionada por el mismo.

Para el primer simulacro, el día 10 de Junio, se realizaron pruebas volumétricas y ataques al sistema a nivel infraestructura, no logrando comprometer la disponibilidad de los activos.

Para el segundo simulacro, el día 17 de Junio, se diseñaron pruebas específicas de carga sobre la aplicación y mediante ataques a configuraciones vulnerables identificadas, fue posible comprometer parcialmente la disponibilidad de uno de dos sistemas responsables de la publicación de resultados. Los hallazgos mencionados, fueron evaluados y atendidos por el proveedor del Sistema Informático PREP. Como resultado de estas pruebas, se identificaron hallazgos con impacto en la disponibilidad del sistema en las siguiente categorías:

- **Servidores:** se requiere agregar servidores adicionales para aumentar capacidad de procesamiento de usuarios.
- **Infraestructura de seguridad:** se requiere utilizar un dispositivo intermedio que mitigue conexiones maliciosas.

- **Desarrollo de la aplicación web:** se requiere evaluar las funciones del sistema de presentación de información que envían gran cantidad de información al usuario, ya que pueden ser abusadas por usuarios maliciosos para saturar la transmisión de datos y procesamiento de información del sistema.

Previo al tercer simulacro, el día 24 de Junio, se utilizaron y reajustaron las pruebas previamente diseñadas.

Los resultados respecto a la disponibilidad del sistema fueron superiores a los simulacros anteriores, fue posible comprometer parcialmente la disponibilidad de algunos sistemas de manera imperceptible, sin afectar la operación debido a los controles.

A partir de los hallazgos del tercer simulacro se robustecieron los controles previamente implementados para mejorar la resistencia a ataques a la disponibilidad del servicio.

En conclusión, podemos afirmar que el riesgo de pérdida de disponibilidad ante ataques a la aplicación Sistema Informático del IEE Sonora es bajo.

pentest
herramienta de diagnóstico eficaz

Informe de pruebas de denegación de servicio al sitio de publicación PREP y al sitio principal del OPLE

Versión	Fecha
1.0	25 Junio 2018
1.1	30 Junio 2018

Contenido

Introducción 3

Resultados generales 4

Introducción

En el presente documento se muestran los resultados de las pruebas de denegación de servicio realizadas a la infraestructura que se encuentra expuesta a Internet, donde se alojan los sistemas información del Sistema PREP y el sitio oficial del OPLE.

Resultados generales

Durante los simulacros de los días 10, 17 y 24 de junio del 2018, se realizaron una serie de pruebas de ataques de denegación de servicio con el objetivo de detectar vulnerabilidades en la infraestructura del sistema informático PREP.

De acuerdo al resultado de estas pruebas, código verde emitió una serie de recomendaciones para eliminar dichas vulnerabilidades y mejorar la seguridad de los componentes de la infraestructura del sistema informático PREP, las cuales han sido atendidas en su mayoría por el proveedor de el sistema informático PREP.

Para el primer simulacro, el día 10 de Junio, se realizaron pruebas volumétricas y ataques al sistema a nivel infraestructura, no logrando comprometer la disponibilidad de los activos.

Para el segundo simulacro, el día 17 de Junio, se diseñaron pruebas específicas de carga sobre la aplicación y mediante ataques a configuraciones vulnerables identificadas, fue posible comprometer parcialmente la disponibilidad de uno de dos sistemas responsables de la publicación de resultados. Los hallazgos mencionados, fueron evaluados y atendidos por el proveedor del Sistema Informático PREP. Como resultado de estas pruebas, se identificaron hallazgos con impacto en la disponibilidad del sistema en las siguiente categorías:

- **Servidores:** se requiere agregar servidores adicionales para aumentar capacidad de procesamiento de usuarios.
- **Infraestructura de seguridad:** se requiere utilizar un dispositivo intermedio que mitigue conexiones maliciosas.

- **Desarrollo de la aplicación web:** se requiere evaluar las funciones del sistema de presentación de información que envían gran cantidad de información al usuario, ya que pueden ser abusadas por usuarios maliciosos para saturar la transmisión de datos y procesamiento de información del sistema.

Previo al tercer simulacro, el día 24 de Junio, se utilizaron y reajustaron las pruebas previamente diseñadas. Los resultados respecto a la disponibilidad del sistema fueron superiores a los simulacros anteriores, aunque fue posible comprometer parcialmente la disponibilidad de algunos sistemas de manera imperceptible, los controles adicionales implementados por el proveedor del Sistema Informático PREP mejoraron considerablemente el desempeño y disponibilidad.

A partir de los hallazgos del tercer simulacro se robustecieron los controles previamente implementados para mejorar la resistencia a ataques a la disponibilidad del servicio.

En conclusión, podemos afirmar que el riesgo de pérdida de disponibilidad ante posibles ataques volumétricos de 3Gbps o menos a la aplicación Sistema Informático del PREP Sonora es bajo.

Después del análisis tecnológico realizado al sitio principal del OPLE, se detectaron vulnerabilidades de configuración, desarrollo de la aplicación e infraestructura con impacto en la disponibilidad.

A partir de estos hallazgos se realizaron modificaciones en las protecciones y controles de seguridad de red existentes, capacidad de los servidores y código fuente del sitio principal para mitigar este tipo de ataques.

En conclusión, el riesgo de pérdida de disponibilidad ante posibles ataques al sitio oficial del OPLE es medio, ya que existen protecciones y ajustes de configuración pendientes por evaluar y aplicar por parte del proveedor del servicio de hospedaje del OPLE. Como principal recomendación, se requiere un rediseño a fondo de la arquitectura de servidores donde se tiene hospedado el sitio web para poder realizar las tareas de aseguramiento requeridas por cada uno de los servicios como es el sitio principal para mostrar un riesgo bajo de pérdida de disponibilidad.

pentest
herramienta de diagnóstico eficaz

Estadísticas del tráfico de red generado para ataques de denegación de servicio

Versión	Fecha
1.0	25 Junio 2018
1.1	30 Junio 2018

Contenido

Introducción 3

Estadísticas de tráfico generado 4

Introducción

En el presente documento se muestran las estadísticas de tráfico de red generado durante las pruebas de denegación de servicio realizadas a la infraestructura del sistema PREP durante los simulacros del 10, 17 y 24 de Junio 2018.

Estadísticas de tráfico generado

Durante los 3 simulacros realizados los días 10, 17 y 24 de Junio 2018, se realizaron ataques volumétricos de 3 Gbps al sistema informático PREP, así como ataques a las configuraciones inseguras que pueden comprometer la disponibilidad.

En los simulacros 2 y 3 se generó carga para simular de 1000 a 1500 usuarios concurrentes. El horario de las pruebas a la disponibilidad fue el siguiente:

- Simulacro 1 - 10 Junio 2018 - 16:00 - 17:00 hora Hermosillo
- Simulacro 2 - 17 Junio 2018 - 12:00 - 13:00 hora Hermosillo
- Simulacro 3 - 24 Junio 2018 - 11:00 - 13:00 hora Hermosillo

Para el sitio principal del OPLE se ejecutaron pruebas similares de ataques volumétricos de hasta 2Gbps y de configuración insegura durante el proceso de auditoría.

Fecha	Método	Servidor	Puerto	Tiempo (segundos)	Ancho de banda (Gbps)
24 Junio 2018	RUDY	simulacroson.prepsonora.org.mx	443	600	3000
	RUDY	simulacroson.prepsonora.org.mx	443	600	3000
	DRDoS SYN	simulacroson.prepsonora.org.mx	443	28	3000
	SYN	simulacroson.prepsonora.org.mx	443	300	3000
	Slowloris	simulacroson.prepsonora.org.mx	443	300	3000
	ARME	simulacroson.prepsonora.org.mx	443	578	3000
17 Junio 2018	Slowloris	simulacroson.prepsonora.org.mx	80	241	3000
	ARME	simulacroson.prepsonora.org.mx	80	600	3000
	DRDoS UDP	simulacroson.prepsonora.org.mx	80	600	3000
	RUDY	simulacroson.prepsonora.org.mx	80	600	3000
	DRDoS SYN	simulacroson.prepsonora.org.mx	80	600	3000
	SYN	simulacroson.prepsonora.org.mx	80	600	3000

Fecha	Método	Servidor	Puerto	Tiempo (segundos)	Ancho de banda (Gbps)
10 Junio 2018	DRDoS CHARGEN	170.247.130.192	N/A	138	3000
	SYN	simulacroson.prepsonora.org.mx	443	15	3000
	DRDoS SYN	simulacroson.prepsonora.org.mx	80	600	3000
	UDP-Lag	simulacroson.prepsonora.org.mx	80	300	3000
	RUDY	simulacroson.prepsonora.org.mx	80	600	3000
	Slowloris	simulacroson.prepsonora.org.mx	80	192	3000
	RUDY	simulacroson.prepsonora.org.mx	80	300	3000
	DRDoS CHARGEN	170.247.130.192	N/A	163	3000

Fecha	Método	Servidor	Puerto	Tiempo (segundos)	Ancho de banda (Gbps)
30 Junio 2018	RUDY	ieesonora.org.mx	443	518	3000
	DRDoS SYN	www.ieesonora.org.mx	443	293	3000
	SYN	ieesonora.org.mx	443	409	3000
	DRDoS CHARGEN	ieesonora.org.mx	x	435	3000
	DRDoS DNS	ieesonora.org.mx	443	114	2090
	DRDoS DNS	ieesonora.org.mx	80	300	2000
	DRDoS SYN	www.ieesonora.org.mx	443	293	3000
29 Junio 2018	RUDY	ieesonora.org.mx	80	300	3000
	DRDoS CHARGEN	ieesonora.org.mx	x	277	3000
	SYN	ieesonora.org.mx	80	68	3000

Fecha	Método	Servidor	Puerto	Tiempo (segundos)	Ancho de banda (Gbps)
1 Julio 2018	DRDoS SYN	ieesonora.org.mx	110	600	2000
	DRDoS SYN	ieesonora.org.mx	110	600	2000
	DRDoS SYN	ieesonora.org.mx	443	51	2000
	DRDoS SYN	ieesonora.org.mx	80	110	2000
	RUDY	ieesonora.org.mx	80	474	2000
	SYN	ieesonora.org.mx	80	132	2000
	DRDoS CHARGEN	ieesonora.org.mx	x	600	2000