

CIBERSECURITY CONSULTING

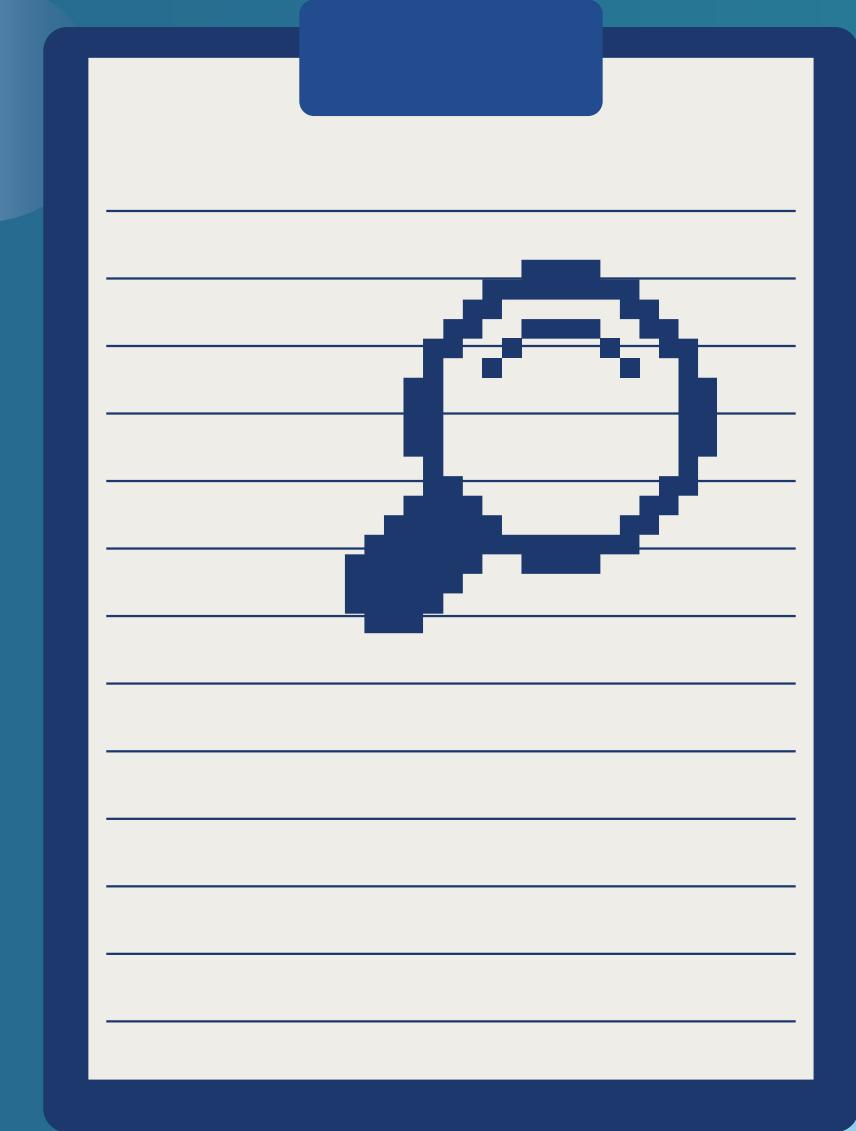
REDES Y PROTOCOLOS
DE COMUNICACIÓN



GRUPO 3: DANIEL H.G., ABEL G.D., JOSE M^a E.P.

ÍNDICE

- Nuestro objetivo
- Metodología de investigación
- Categorías y ejemplos con medidas propuestas
- Conclusión



NUESTRA MISIÓN

Proteger a TrustShield Financial

Nuestra empresa, TrustShield Financial, nos ha pedido realizar un análisis completo de su infraestructura de redes. Piénsalo como una revisión médica para la red de la compañía.

El Objetivo Principal

Nuestro objetivo es encontrar las "grietas" o vulnerabilidades más importantes que podrían poner en peligro la información financiera. Queremos asegurarnos de que los datos estén siempre seguros (confidencialidad), no sean alterados (integridad) y estén disponibles cuando se necesiten (disponibilidad).



Fase 1: Categorías

Estudiamos los tipos generales de vulnerabilidades que existen en redes, como si aprendiéramos las diferentes familias de problemas.

Fase 2: Ejemplos

Investigamos vulnerabilidades específicas y conocidas (llamadas CVEs) que encajan en esas categorías.

Fase 3:Medidas propuestas

Analizamos formas de salvaguardar esas vulnerabilidades

METODOLOGÍA DE INVESTIGACIÓN

Hemos dividido nuestro trabajo en tres fases claras para abordar el problema de manera ordenada y eficaz.



VULNERABILIDAD:PROTOCOLOS CRIPTOGRÁFICOS

CVE-2014-0160 (HEARTBLEED)

5/15



Descripción breve

Fallo en la extensión 'Heartbeat' de la librería OpenSSL que permite a un atacante leer fragmentos de la memoria del servidor.

En palabras sencillas

Cuando te conectas a una web segura, se envían 'latidos' para confirmar que la conexión sigue activa. Este fallo permitía a un atacante pedir un 'latido' y decir 'dame una respuesta de 1000 letras', pero enviando solo 1. El servidor, confundido, devolvía las 999 letras siguientes que tuviera en su memoria, que podían ser las contraseñas de otros usuarios.

impacto

Fuga masiva de información sensible como contraseñas, cookies de sesión y, lo más grave, las claves privadas del servidor.

EXPLORACIÓN

Envío de una petición malformada que solicita una respuesta aunque envía pocos datos, haciendo que el servidor devuelva información

CONTRAMEDIDA PROPUESTA

Actualizar la librería OpenSSL a una versión parcheada, y revocar y regenerar todos los certificados y claves privadas que pudieran haber sido expuestos.

VULNERABILIDAD: AMPLIFICACIÓN Y REFLEXIÓN UDP

6/15

CVE-2018-1000115 (MEMCACHED)

Descripción breve

Permite usar servidores Memcached mal configurados (con el puerto UDP 11211 expuesto) para lanzar ataques de denegación de servicio (DDoS) con un factor de amplificación altísimo.

En palabras sencillas



Un atacante envía una postal a miles de bibliotecas pidiendo 'envíen la enciclopedia completa a esta dirección', poniendo la dirección de la víctima. Las bibliotecas, obedientes, envían miles de camiones cargados de libros a la puerta de la víctima, colapsando por completo su calle y dejándola inaccesible.

Explotación

Envío de una petición malformada que solicita una respuesta aunque envía pocos datos, haciendo que el servidor devuelva información

Impacto

DDoS de gran volumen que pueden saturar y desconectar a grandes infraestructuras de red.

CONTRAMEDIDA PROPUESTA

Actualizar Memcached, deshabilitar el soporte UDP si no es necesario y filtrar el puerto 11211 en el perímetro de la red.

VULNERABILIDAD: ACCESO REMOTO INSEGURO

CVE-2019-0708 (BLUEKEEP)

7/15

Descripción breve

Vulnerabilidad crítica en los Servicios de Escritorio Remoto (RDP) de Windows que permite ejecución remota de código sin autenticación.

Impacto

Compromiso total de servidores Windows (confidencialidad, integridad y disponibilidad). Es 'wormable', puede propagarse sola.



En palabras sencillas

Piensa en el 'Escritorio Remoto' como una puerta para controlar un ordenador a distancia. Este fallo es como descubrir que esa puerta tiene una cerradura rota de fábrica. Un atacante puede enviar una 'llave' especial que abre la puerta de par en par, sin necesidad de contraseña, y tomar el control completo del servidor.

Explotación

Envío de peticiones RDP especialmente diseñadas a sistemas vulnerables y sin parchear.

CONTRAMEDIDA PROPUESTA

Aplicar el parche de seguridad de Microsoft, habilitar la Autenticación a Nivel de Red (NLA) y no exponer el puerto RDP (3389) a internet.

VULNERABILIDAD: PROTOCOLOS DE GESTIÓN

8/15

CVE-2024-3661 (TUNNELVISION)

Descripción breve

Ataque donde un servidor DHCP (asigna direcciones IP automáticas) malicioso inyecta rutas en clientes de la misma red local.

IMPACTO

Rompe la confidencialidad de la VPN: tráfico observado y posibilidad de redirigirlo por el atacante

EXPLOTACIÓN

Por ejemplo en una Wi-Fi pública el atacante crea una red falsa para manipular los dispositivos conectados.

CONTRAMEDIDA PROPUESTA

Usar clientes VPN de confianza y seguras contra este problema y evitar redes Wi-Fi no confiables.



En palabras sencillas

Alguien en la misma red puede manipular a tu equipo para que deje de usar la VPN y ver tu tráfico.

VULNERABILIDAD: COMPARTICIÓN DE ARCHIVOS

9/15

CVE-2017-0144 (ETERNALBLUE)

Server Message Block

Descripción breve

Vulnerabilidad crítica en el protocolo SMBv1 (usado para compartir archivos en Windows entre dispositivos de una red) que permite ejecución remota de código.

IMPACTO

Base de ataques de ransomware. Permite movimiento lateral y propagación automática en la red.

EXPLOTACIÓN

Envío de paquetes de red específicamente diseñados a servidores que usan protocolo SMBv1.

CONTRAMEDIDA PROPIA

Deshabilitar por completo el protocolo SMBv1 en todos los sistemas y segmentar la red para contener la propagación.



En palabras sencillas

Fallo en una función antigua de Windows permitía que un virus se extendiera solo por toda la red.

VULNERABILIDAD: BUGS EN PILAS TCP/IP

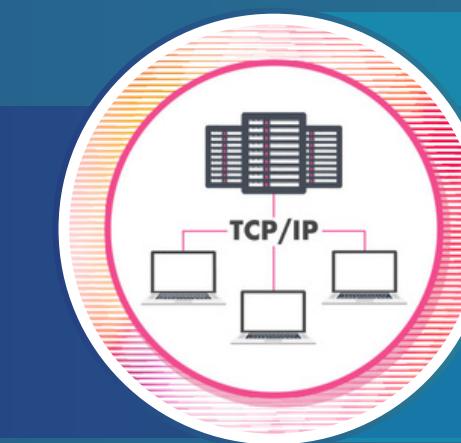
10/15

CVE-2019-12255 (URGENT/11)

Descripción breve

Descripción: Error de gestión del puntero de urgencia TCP en la pila IPnet utilizada por VxWorks que posibilita la ejecución remota de código (RCE).

En palabras sencillas



Es un fallo grave en VxWorks que permite que, con mensajes de red especialmente preparados, alguien tome control del dispositivo sin contraseña; afecta a muchos equipos embebidos y se corrige instalando las actualizaciones del fabricante.

IMPACTO

Acceso administrativo remoto

EXPLORACIÓN

Obtener el número de serie (físicamente o por red) y usarlo para calcular la contraseña de fábrica.

CONTRAMEDIDA PROPUESTA

Envío de paquetes TCP especialmente formados que desencadenan el fallo



VULNERABILIDAD: CONFIGURACIONES INSEGURAS

11/15

CVE-2024-51978 (IMPRESORAS)

Descripción breve

Permite a un atacante generar la contraseña de administrador por defecto a partir del número de serie de la impresora.

IMPACTO

Acceso administrativo remoto

EXPLORACIÓN

Obtener el número de serie (físicamente o por red) y usarlo para calcular la contraseña de fábrica.



En palabras sencillas

En ocasiones, equipos como las impresoras no se configuran adecuadamente, permitiendo la entrada de atacantes al poder conseguir la contraseña de administrador de la impresora.

CONTRAMEDIDA PROPIETA

Envío de paquetes TCP especialmente formados que desencadenan el fallo

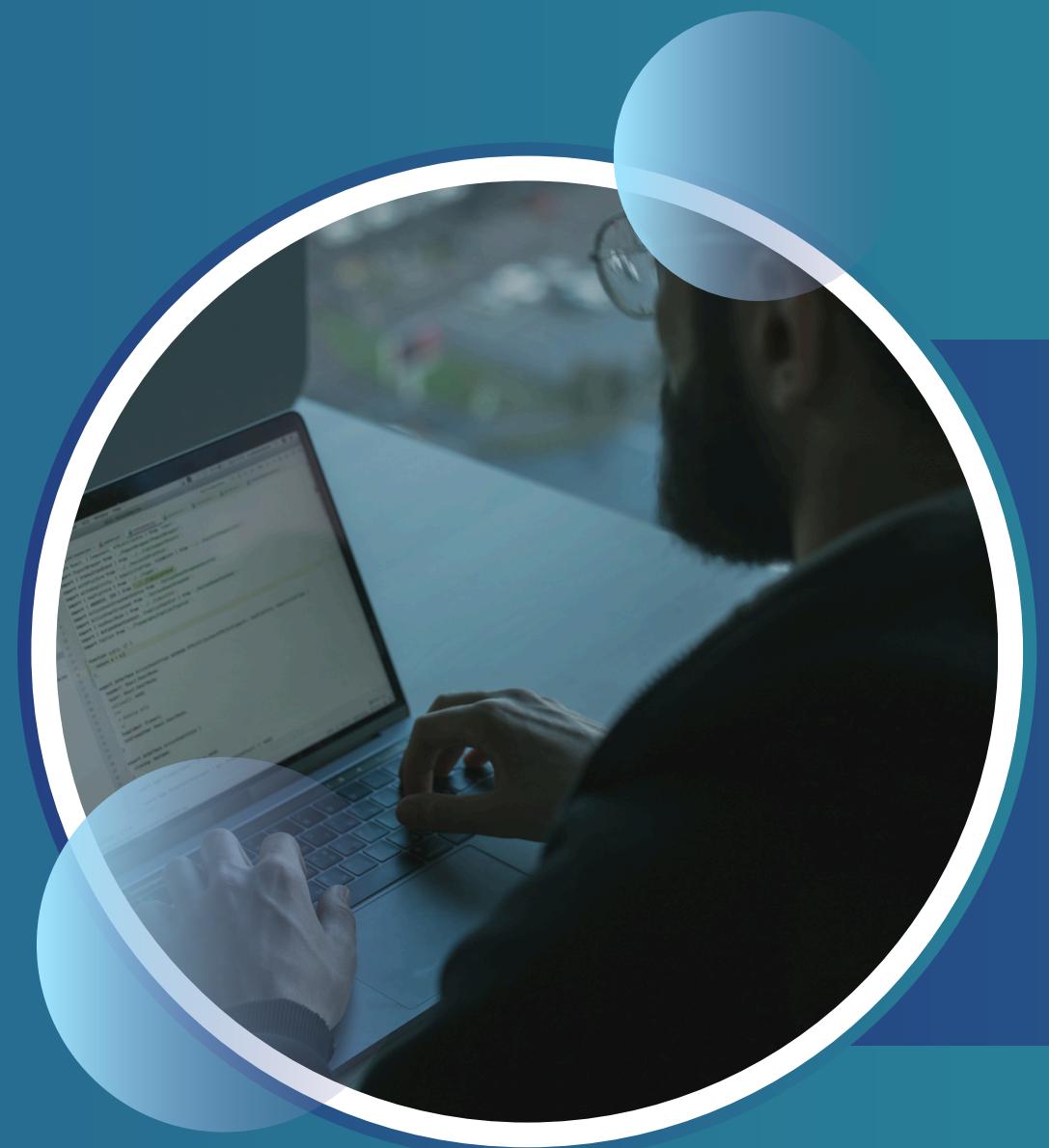


CONCLUSIÓN

Nuestro análisis exhaustivo revela que muchas de las amenazas más críticas que enfrenta TrustShield Financial persisten debido a fallos en la higiene básica de ciberseguridad: sistemas sin parches, configuraciones por defecto y una segmentación de red insuficiente.

Recomendación Final

La implementación rigurosa del plan de contramedidas propuesto, basado en los tres pilares de actualización, fortalecimiento y segmentación, permitirá a la organización fortalecer drásticamente la confidencialidad, integridad y disponibilidad de su información, reduciendo significativamente la superficie de ataque y mejorando su resiliencia frente a futuros incidentes.



**GRACIAS POR SU
ATENCIÓN**

¿ALGUNA PREGUNTA?

