**Informe Seguridad**

[nicolas aspes cuadra](mailto:nicolas.aspes.c@mail.pucv.cl)/ gustavo camus maturana

**Introducción**

Se detectaron 2 Vulnerabilidades que podrían explotar y poner en riesgo los datos de la compañía y de los usuarios, robando información o la infiltración de Software malicioso.

**Explicación**

Hemos detectado que nuestro servidor es fácilmente accesible usando nuestra dirección **IP (172.217.12.116)** del servidor, con el uso de **OWASP ZAP**, detectando 2 amenazas para nuestro servidor pueden ser peligrosas para la seguridad de la empresa y de los usuarios.

**Problema**

Las 2 amenazas encontradas en el servidor son dos puertos abiertos **(443 y 80).**

Esto podría llegar a vulnerabilidades que pueden afectar al servidor en gran medida si no se hace algo para detener un posible ataque o un robo de datos y una posible amenaza interna debido a empleados malintencionados o con falta de conocimientos básicos de Seguridad informática.

**Consecuencias**

El principal riesgo es la exposición de servicios y datos a posibles atacantes que pueden explotar la vulnerabilidad obteniendo acceso no autorizado a la red y los datos e introducir Software maliciosos, malware e ingeniería social para extorsionar a usuarios o trabajadores de compañía.

**Solución**

### **Cerrar los puertos que no sean necesarios**

determina si realmente es necesario que esté accesible. Si un servicio no se usa o no necesita estar expuesto a internet o a otros equipos de la red, lo mejor es desactivarlo.

### **Limitar el acceso a los puertos importantes**

Para los puertos que sí necesitas (como el puerto del servidor web o SSH), permite solo que ciertas direcciones IP o rangos de IP confiables se conecten a ellos.

### **Hacer revisiones y auditorías periódicas**

Cada cierto tiempo, revisa de nuevo qué puertos tienes abiertos y actualiza tus políticas de seguridad según las necesidades actuales del sistema.

### **Implementar sistemas de monitoreo y alertas**

Configura herramientas que te avisen si algún puerto se abre de forma inesperada o si hay intentos de conexión sospechosos.