

Documentacion Proyecto tunn



FIN.0039. Credenciales por defecto activadas

Vulnerabilidad

Se encuentran credenciales por defecto de baja fortaleza las cuales an estn presentes en la base de datos de la aplicacin.

Donde

GeoVision inc, gestor de camaras (3) admin:admin

Servicio Polycom de llamadas centralizadas (1) admin:admin

Recursos compartidos (4) administrator:password

SQL server database (2) sa:sa sa:password

Dispositivos Cisco AP y Switches (5) Cisco:Cisco cisco:cisco

Firebird Database (1) SYSDBA:masterkey

Recomendacion

Eliminar las credenciales del gestor de almacenamiento para evitar inicios de sesin con estas. = Documentacion Proyecto tunn

FIN.0020. Uso de canal inseguro

Vulnerabilidad

La informacin de los clientes es transmitida por un canal que no usa cifrado, por lo cual puede ser capturada en texto plano credenciales e informacin confidencial.

Donde

- uso de office 365 de escritorio el cual se comunica por HTTP (2)
- Aplicacin para monitoreo de redes (1)

Recomendacion

Desplegar la aplicacin sobre un canal de comunicacin cifrado, como por ejemplo: HTTPS + TLS. = Documentacion Proyecto tunn

FIN.0048. adivinidas

Claves

debiles

Vulnerabilidad

La falta de complejidad de las contraseas reduce significativamente el tiempo de bsqueda cuando se trata de adivinar las contraseas de los usuarios, por lo que un atacante puede realizar un ataques de fuerza bruta y tener xito ms rpido.

Donde

usuarios del directorio activo con contrasea dbil (7)

Recomendacion

Hacer cumplir el uso de contraseas seguras. Una poltica de seguridad de la contrasea debe contener los siguientes atributos: - Configurar una longitud mnima y mxima - Exigir conjuntos de carcteres mixtos (alfanumrico, casos especiales, mixta) - No contener nombres de usuario. - No reutilizar contraseas. = Documentacion Proyecto tunn

FIN.0036. Fuga de informacin de negocio

Vulnerabilidad

Se obtiene informacin de negocio, como: - Facturas. - Recaudos. - Generacin de ordenes de servicio. - Creacin de contratos.

Donde

Acceso al mdulo donde se encuentran todas las facturas del negocio (1)

Recomendacion

De acuerdo a la clasificacin de la informacin encontrada, establecer los controles necesarios para que la informacin sea accesible solo a las personas indicadas. = Documentacion Proyecto tunn

FIN.0024. Enumeracin de usuarios

Vulnerabilidad

Los nombres de los equipos de Red son los mismos que los usuarios del AD, esto permite mediante un escaneo identificar usuarios registrados.

Donde

10.122.16.1 10.127.23.1

Recomendacion

Implementar mensajes de error genricos que no le permitan a un atacante discernir la existencia del usuario en el sistema a travs de los errores HTTP (500 o 404) .