Documentacion Proyecto macall

FLUID

SECURITY WITHOUT MYSTERY

FLUID

FIN.0050. Algoritmo de cifrado inseguro

Vulnerabilidad

El servidor, soporta un cifrado dbil en el protocolo SMB , al igual que el protocolo RDP. Esto hace que el riesgo aumente debido a que estos tipos de cifrado son considerados como vulnerables.

Amenaza

Un usuario desde un segmento autorizado puede realizar un ataque de hombre en el medio (MiTM) e interceptar la informacin transmitida.

Riesgo

Probabilidad de que un usuario desde un segmento autorizado pueda realizar un ataque de hombre en el medio y pueda descifrar la informacin transmitida.

Donde

10.8.69.173 445 10.8.69.173 3389

Recomendacion

Solamente se debe de permitir cifrados seguros con algoritmos seguros como TLSv1 o Superior. = Documentacion Proyecto macall

FIN.0037. Uso de web services sin autorizacin

Vulnerabilidad

Es posible hacer peticiones al web service sin estar logueado en la aplicacin para

crear o consultar llaves del audiovalor.

Amenaza

Un usuario malintencionado desde la intranet puede consumir los webservices y realizar ataques de fuerzabruta con el fin de hallar credenciales y posteriormente generar o consultar laves del audiovalor.

Riesgo

Probabilidad de que un un usuario malintencionado desde la intranet puede consumir los webservices y realizar ataques de fuerzabruta con el fin de hallar credenciales y posteriormente generar o consultar laves del audiovalor.

Donde

http//10.8.69.17372/IntermediaWSseguridad/AudiovalorGeneracionLlave.asmx

http//10.8.69.17372/IntermediaWSseguridad/AudioValorLlave.asmx

Recomendacion

Implementar Tokens para validar cada peticin que se haga a los webservices - Cifrar la informacin sensible. -impelementar autorizacin para evitar el uso de los web services pblicamente. = Documentacion Proyecto macall

FIN.0051. Ausencia de proteccin contra ataques de fuerza bruta

Vulnerabilidad

La aplicacin no tiene proteccin contra ataques de automatizados para adivinar credenciales validas.

FLUID

Amenaza

Un usuario no autorizado con acceso a la intranet puede enumerar cuentas y claves de usuarios vlidos a travs de un robot elaborado que ejecute ataques de fuerza bruta y diccionario.

Riesgo

Probabilidad que una o varias cuentas de la aplicacin sean robadas o enumeradas por un robot debido que el sistema no valida que quien se intenta autenticar sea un humano, lo que puede afectar la disponibilidad de las cuentas vulneradas y la trazabilidad de sus acciones en el sistema.

Donde

-http://10.8.69.173:72/IntermediaWSseguridad/AudioValorLlave.asmx

-http://10.8.69.173:72/IntermediaWSseguridad/AudiovalorGeneracionLlave.asmx

-10.8.69.173 445

Recomendacion

Implementar un control para evitar este tipo de ataques y que garantice que el acceso no sea de un robot. Ej captcha, bloqueo por retardo en el nmero de intentos fallidos, etc. = Documentacion Proyecto macall

FIN.0038. Webservices expuestos

Vulnerabilidad

El servidor tiene los web services expuestos, lo que permite que cualquier empleado de la organizacin pueda ingresar y tratar de generar o consultar una llave para el Audiovalor.

Amenaza

Un usuario malintencionado desde la intranet puede ingresar a las url de los web services y realizar ataques de fuerza bruta para hallar credenciales y poder generar o consultar llaves del audiovalor.

Riesgo

Probabilidad de que un usuario malintencionado desde la intranet pueda ingresar a las url de los web services y realizar ataques de fuerza bruta para hallar credenciales y poder generar o consultar llaves del audiovalor.

Donde

http//10.8.69.17372/IntermediaWSseguridad/AudiovalorGeneracionLlave.asmx

http//10.8.69.17372/IntermediaWSseguridad/AudioValorLlave.asmx

Recomendacion

Implementar autenticacin para visualizar los webservices o en su defecto eliminar su acceso pblico. = Documentacion Proyecto macall

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.

Amenaza

Un usuario no autorizado puede interceptar el canal HTTP para hacer un Man in the Middle capturando as todo el trfico de red con informacin sensible.

FLUID

Riesgo

Probabilidad de que un usuario no autorizado intercepte el canal donde se genera el trfico de la aplicacin permitiendo as la lectura de este.

Donde

http//10.8.69.173 72/

Recomendacion

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

FIN.0047. Certificados Digitales Inseguros

Vulnerabilidad

El certificado no cumple con las mejores prcticas recomendadas, en este caso se encuentra autofirmado y no posee la garanta de una entidad de confianza que permita certificar que el servidor realmente sea.

Amenaza

Un usuario desde un segmento autorizado puede realizar un ataque de hombre en el medio y hacerse pasar por el servidor que procesa los web services para interceptar la informacin.

Riesgo

Probabilidad de que un usuario desde un segmento autorizado mediante un ataque de hombre en el medio, pueda interceptar la informacin transmitida entre un cliente y el servidor que procesa los web services, con el fn de modificar los datos enviados, capturar credenciales,etc.

FLUID

Donde

10.8.69.173 3389

Recomendacion

Generar un certificado firmado por una entidad interna vlida y de confianza. = Documentacion Proyecto macall

FIN.0035. Fuga de informacin tcnica

Vulnerabilidad

Se obtiene informacin tcnica del sistema, como: - versin de los componentes que el sistema utiliza (encabezados HTTP, banner del servicio, etc) - informacin especfica sobre la configuracin componentes a nivel del servidor.

Amenaza

Un usuario no autorizado desde la Intranet con acceso al sistema puede identificar versiones y/o componentes que usa el sistema a travs de las cabeceras HTTP que responde el servidor o en la respuesta a los errores HTTP no personalizados.

Riesgo

Probabilidad que un usuario no autorizado desde intranet obtenga informacin tcnica del servidor y sus componentes para preparar un ataque ms elaborado debido que la configuracin actual del sistema expone informacin de versiones y componentes.

Donde

http://10.8.69.173 10.8.69.173 445

FLUID

Recomendacion

Eliminar el banner de los servicios con fuga de informacin, Verificar que los encabezados HTTP no expongan ningun nombre o versin. = Documentacion Proyecto macall

FIN.0041. Cabeceras de seguridad HTTP no establecidas

Vulnerabilidad

El servidor carece de algunos encabezados HTTP que le permiten evitar ataques como el clickjacking y Cross site Scripting a las pginas que estn alojadas en ste.

Amenaza

Un usuario en la intranet puede realizar ataques como clickjacking y XSS pudiendo modificar el contenido que se le presenta a los usuarios de la aplicacin debido a que no se est estableciendo las cabeceras de seguridad.

Riesgo

Probabilidad de que un usuario en la intranet pueda modificar el contenido que se le presenta a los usuarios debido a que no se tienen definidas las cabeceras de seguridad, lo que puede ocasionar robo de informacin de los usuarios, as como la distribucin de software malicioso.

Donde

HTTP Strict Transport Security (HSTS) Public Key Pinning Extension for HTTP (HPKP) X-Frame-Options X-XSS-Protection X-Content-Type-Options Content-Security-Policy X-Permitted-Cross-Domain-Policies

FLUID

Recomendacion

Establecer las cabeceras HTTP de seguridad: - access-control-allow-origin - x-content-security-policy - x-permitted-cross-domain-policies - strict-transport-security (Si usa SSL) - x-frame-options - x-xss-protection - cache-control.