REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

Organización	BANVIVIENDA
Fecha	27/11/2018
Servicio	MSS-VME
Nivel de Severidad	Medio
Nivel de Impacto	Medio
Nivel de Vulnerabilidad	Medio

DESCRIPCION DE INCIDENTE

Nuestro Centro de Operaciones le presenta un resumen de las vulnerabilidades presentes en sus sistemas.

- Host 200.46.19.100: Detección de SSL versión 2 y 3, vulnerabilidad de SSL v3 POODLE, vulnerabilidad de Suite de Cifrado RC4 en SSL Bar Mitzvah.
- Host 200.46.227.227: Modo agresivo en IKE con llave pre-compartida.
- 200.46.227.230: Detección de SSL versión 2 y 3, detección de suites de cifrado de fuerza débil, detección de suites de cifrado de fuerza intermedia, vulnerabilidad en SSLv2 DROWN, vulnerabilidad de Suite de Cifrado RC4 en SSL Bar Mitzvah.
- Host 200.90.137.83: Detección de suites de cifrado de fuerza intermedia, certificado SSL no es de confianza.
- 200.90.137.84: Detección de suites de cifrado de fuerza intermedia, detección de módulos Diffie-Hellman menor a 1024 bits LOGJAM.
- 200.90.137.94: Detección de suites de cifrado de fuerza intermedia, divulgación de información por el Client Access Server de Exchange, vulnerabilidad de Suite de Cifrado RC4 en SSL Bar Mitzvah.

SSL v2 y v3 han sido declarados protocolos inseguros debido a numerosas debilidades que presentan, permitiendo a un atacante realizar ataques de hombre el en medio o descifrar la información que hace uso de estos protocolos.

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

Las vulnerabilidades POODLE y DROWN afectan a SSLv3 y SSLv2 respectivamente, cualquier implementación de estos protocolos es afectada por estas vulnerabilidades, por lo que se recomienda no utilizar los protocolos mencionados.

Las suites de cifrado que tengan longitud de llave entre 64 y 112 bits o que utilicen 3DES se consideran de fuerza intermedia, sin embargo, este tipo de suites de cifrado es considerado débil para estándares modernos, un ejemplo de suite de cifrado fuerte moderno es TLS 1.2 con AES-GCM.

El uso de módulos de Diffie-Hellman inferior a 1024 bits puede permitir a los atacantes encontrar el secreto compartido en un periodo corto de tiempo utilizando criptoanálisis, obteniendo la información de la conexión en texto plano.

El uso de llaves pre-compartidas en modo agresivo del protocolo IKE permite que un atacante pueda capturar un paquete y trate de *crackear* la llave pre-compartida del Gateway de la VPN.

La vulnerabilidad del CAS de Exchange permite a un atacante remoto obtener la dirección IP interna del servidor.

ACCIONES A TOMAR

Para la vulnerabilidad de Exchange la aplicación de parches del fabricante corrige la vulnerabilidad.

Se recomienda utilizar TLS 1.2 en vez de SSL en todas las conexiones que deben ser aseguradas, TLS 1.2 es el protocolo mínimo recomendado que es considerado seguro hoy día.

Para el protocolo IKE se recomienda desactivar el modo agresivo si se utilizan llaves pre-compartidas.

COMENTARIOS Y RECOMENDACIONES

- Se recomienda mantener todo el software actualizado para corregir vulnerabilidades

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

presentes en versiones viejas.

- Si no es posible desactivar el modo agresivo en el protocolo IKE, se recomienda utilizar llaves pre-compartidas fuertes e impedir conexiones a la VPN de hosts no autorizados.
- Se debe deshabilitar SSL y habilitar TLS 1.2 como mínimo.

PROTOCOLO DE COMPARTICION DE INFORMACION DE GLESEC

LOS REPORTES DE INCIDENCIAS DE CYBERSEGURIDAD DE GLESEC están en cumplimento con el protocolo de Semáforo (TLP) del Departamento de Seguridad de Estado de Estados Unidos (DHS): TLP -Blanco (Divulgación no limitada), TLP-Verde (Divulgación Limitada, Restringida, solo para la comunidad), TLP-Ámbar (Divulgación Limitada, Restringida, Para los participantes de la Organización) y TLP-Rojo (No Divulgación, Restringida/Confidencial – Solo compartida con el US DHS).