REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

Organización	COPA AIRLINES
Fecha	23/10/2018
Servicio	MSS-VME
Nivel de Severidad	Crítico
Nivel de Impacto	Crítico
Nivel de Vulnerabilidad	Crítico

DESCRIPCION DE INCIDENTE

Nuestro Centro de Operaciones encontró varias vulnerabilidades detalladas a continuación, que afectan al host 200.46.240.139. La primera vulnerabilidad, es una conocida de severidad crítica, donde se detectó un servidor IIS 6.0 instalado. Esta es una versión muy antigua y es considerada vulnerable a distintos tipos de ataques.

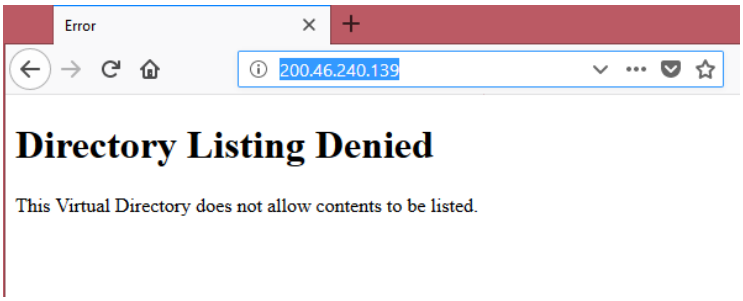
Otra vulnerabilidad detectada es la versión del sistema operativo que se está ejecutando en este servidor es Windows Server 2003. El soporte extendido de Microsoft para esta versión de Windows expiró el 14 de julio de 2015, por lo que ya no se desarrollan parches para esta versión de Windows, haciendo que este sistema operativo sea vulnerable a ataques existentes y expuesto a ataques que se desarrollen en un futuro.

Otra vulnerabilidad presente en este servidor es la HTTP OPTIONS Method Enabled. Esta vulnerabilidad se detectó en el puerto 80. Tener el método HTTP OPTIONS habilitado permite que el servidor Web exponga que otros métodos son soportados por el servidor Web permitiendo que los atacantes puedan obtener más información acerca del servidor, y así puedan concentrar sus esfuerzos en un objetivo en particular.

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

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR



ACCIONES A TOMAR

Verificar si este servicio (IIS 6.0) se encuentra configurado en este sistema, verificar si existe disponibilidad de la página web dentro de la red interna, en caso de que este servicio no sea necesario o no este en uso remover este servicio del sistema. En caso de que se piense utilizar este equipo como servidor web se debe actualizar a la versión más reciente de IIS.
Para la vulnerabilidad de HTTP OPTIONS, es recomendable deshabilitar este método, el procedimiento para deshabilitar dependerá del servidor.
También es recomendable actualizar la versión de Windows Server a uno que tenga soporte oficial y aplicar las actualizaciones de seguridad, en caso de que este equipo se utilice como servidor web.

COMENTARIOS Y RECOMENDACIONES

Siguiendo el principio del mínimo privilegio se debe tomar en cuenta que servicios que estén en desuso, deben estar deshabilitados para reducir el riesgo de que un usuario con malas intenciones intente causar un impacto negativo en la organización. GLESEC recomienda que se mitigue la misma en el menor tiempo posible.

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

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

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).