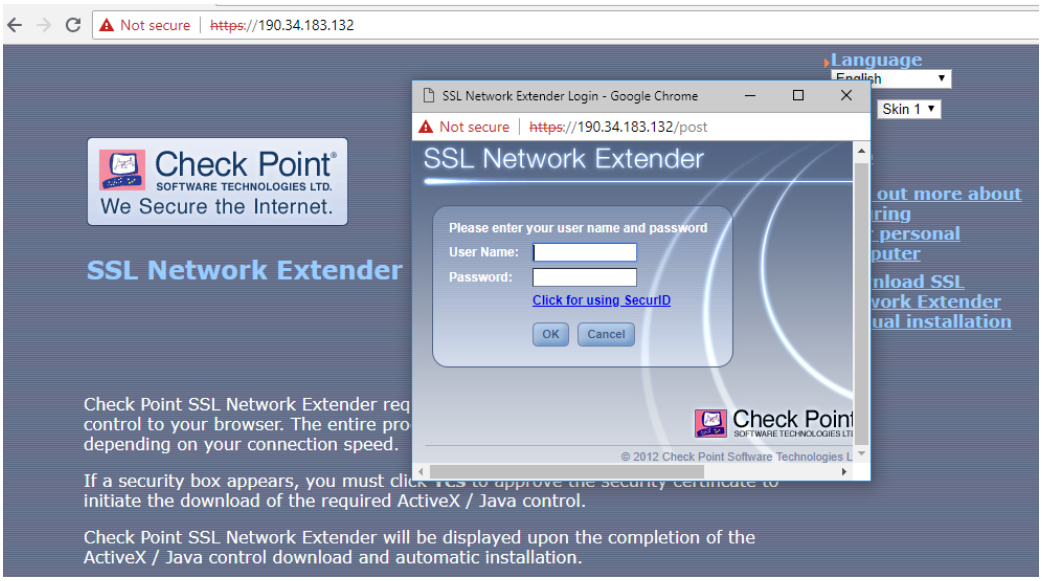
REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

Organización	METROBANK
Fecha	12/07/2018
Servicio	MSS-VM
Nivel de Severidad	High
Nivel de Impacto	High
Nivel de Vulnerabilidad	High

DESCRIPCION DE INCIDENTE

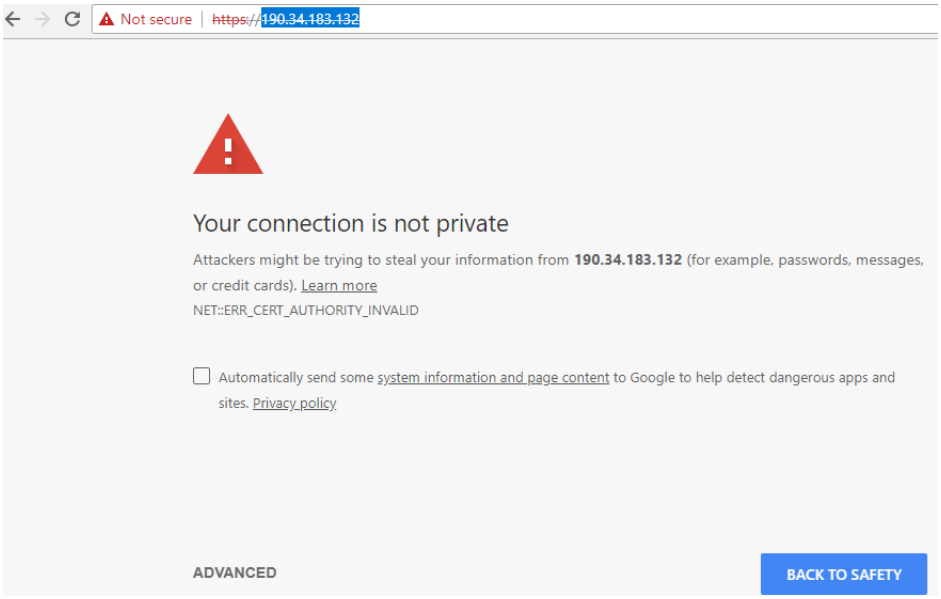
Nuestro Centro de Operaciones encontró que está disponible el servicio SSL Network Extender de Checkpoint en el host IP 190.34.183.132, por lo cual nos gustaría saber si el cliente-miembro METROBANK esta anuente a esto y también al riesgo que puede representar la utilización de este tipo de servicios de acceso remoto, más aún, porque nuestra inteligencia muestra que esta dirección lógica ha sido objetivo de una cantidad considerable de ataques informáticos los cuales han sido bloqueados, sin embargo, este hecho representa una amenaza.



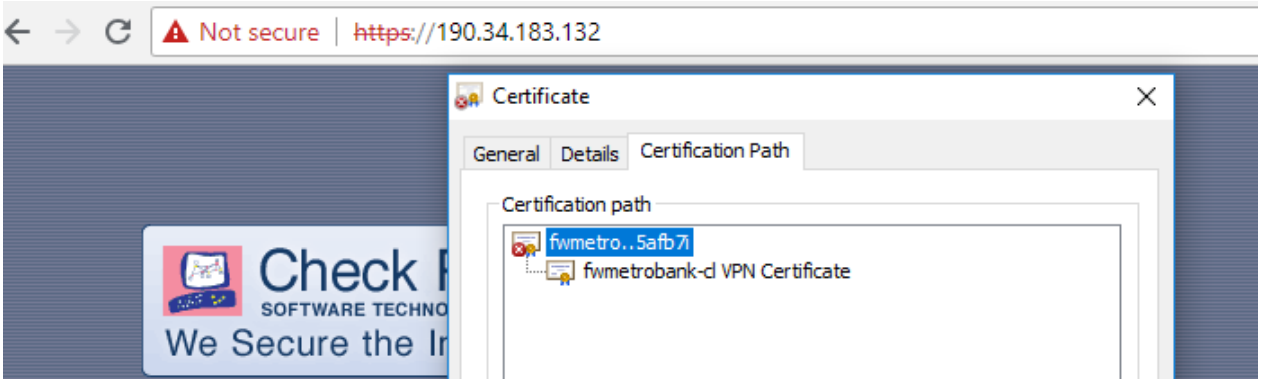
REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

Otro punto que vale la pena destacar es el hecho de que el certificado digital con el que cuenta este servicio WEB es invalido, esto se considera una vulnerabilidad alta ya que el Cliente puede ser objetivo de ataques de suplantación de identidad.



El motivo por el cual este certificado se cataloga como invalido es debido a que la autoridad certificadora (CA) con que fue emitido el mismo no es reconocida como una CA confiable como se muestra a continuación



REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

ACCIONES A TOMAR

En caso de que no sea estrictamente necesario, deshabilitar el servicio SSL Network Extender de Checkpoint y solamente habilitarlo en el momento que se requiera utilizar.

Renovar el certificado para este servicio web e instalarlo apropiadamente. Este debe ser emitido por una Autoridad Certificadora confiable.

COMENTARIOS Y RECOMENDACIONES

Siempre es recomendable aplicar el principio de mínimo privilegio, el cual indica que todos los servicios y/o aplicaciones que no estén expresamente permitidas deben estar deshabilitadas.

El hecho de contar con certificados emitidos por CAs confiables y válidos, al menos para los servicios externos, brinda un menor nivel de riesgo de que se aplique algún mecanismo de suplantación de identidad en los sistemas expuestos.

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

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

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).

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