REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

Organización	Metrobank, S.A
Fecha	20/08/2018
Servicio	MSS-VME, MSS-APS
Nivel de Severidad	High
Nivel de Impacto	High
Nivel de Vulnerabilidad	High

DESCRIPCION DE INCIDENTE

El Centro de Operaciones encontró que 4 de sus hosts están siendo atacadas y que a su vez se presentan dentro de los hosts más vulnerables. A continuación, se mencionan los tipos de ataque destinados a los mismos en los últimos 20 días y vulnerabilidades que presenta cada host:

El host 190.34.183.149 recibe ataques de tipo: TCP Scan (vertical), TCP handshake violation, primer paquete no es syn, Web Scan, HTTP Page Flood Attack, TCP Flags inválidos y presenta vulnerabilidades como: SSL Medium Strength Cipher Suites Supported, SSL RC4 Cipher Suites Supported, SSL Version 2 and 3 soportada.

El host 190.34.183.131 recibe ataques de tipo: TCP Scan (vertical), **SQL Injection**, HTTP Page Flood Attack, TCP handshake violation, primer paquete no es syn, puerto de origen o destino de capa 4 igual a cero; y presenta la vulnerabilidad MS15-034: en HTTP.sys (KB3042553) que representa una severidad critica. A través de los métodos de comprobación utilizados, los cuales no generan el riesgo de detener el servicio, no se ha podido determinar si esta vulnerabilidad representa o no un falso positivo, para esto seguir el segundo punto de las acciones a tomar.

El host 190.34.183.132 recibe ataques de tipo: network flood IPv4 UDP, TCP handshake violation, primer paquete no es syn, puerto de origen o destino de capa 4 igual a cero, SIP-Scanner-SIPVicious, network flood IPv4 TCP-SYN; y presenta vulnerabilidades como: SSL

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

Certificate Cannot Be Trusted, SSL Certificate Chain Contains RSA Keys Less Than 2048 bits, SSL Certificate Signed Using Weak Hashing Algorithm, SSL Medium Strength Cipher Suites Supported y SSL Self-Signed Certificate.

El host 190.34.183.154 recibe ataques de tipo: TCP handshake violation, primer paquete no es syn, HTTP Page Flood Attack, TCP Flags inválidos, network flood IPv4 UDP y presenta las vulnerabilidades conocidas como: SSL Medium Strength Cipher Suites Supported, SSL RC4 Cipher Suites Supported, SSL Version 2 and 3soortada, SSL Weak Cipher Suites Supported.

ACCIONES A TOMAR

Se recomienda realizar las remediaciones pertinentes por host para cada vulnerabilidad especifica para reducir el nivel de riesgo en sus sistemas.
Revisar si el host 190.34.183.131 cuenta con todas las actualizaciones de seguridad recomendadas por Microsoft, en especial, KB3042553.

COMENTARIOS Y RECOMENDACIONES

El dispositivo DefensePro se encarga de detener todos los ataques mencionados en este reporte, sin embargo, si un atacante es capaz de detectar la presencia de estas vulnerabilidades podría explotarlas, y así causar un impacto negativo en su organización. Es importante destacar la relevancia de los hosts asociados a las direcciones IP mencionadas ya que no solo presentan vulnerabilidades conocidas, sino que también, han sido objetivo de distintos tipos de ataques.

Si ustedes desean utilizar las horas de consultoría para que validemos, de una manera controlada, la existencia de esta vulnerabilidad (en host IP 190.34.183.131), por favor contactar a GLESEC SUPPORT.

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