REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

Organización	Metrobank, SA
Fecha	22/11/2018
Servicio	MSS-VME, MSS-APS y MSS-APFW
Nivel de Severidad	Alto
Nivel de Impacto	Alto
Nivel de Vulnerabilidad	Alto

DESCRIPCION DE INCIDENTE

Como parte de los servicios MSS-VME en correlación con MSS-APS & MSS-APFW y haciendo seguimiento a los incidentes #1183, #1193, #1220 y #1230 en los cuales se reportaron vulnerabilidades en sus sistemas críticos los cuales fueron:

190.34.183.152 (https://www.metrobanksa.com)

190.34.183.131 (https://www.govimar.com.pa),

190.34.183.139 (http://appserver.metrobanksa.com),

190.34.183.149 (https://mail.metrobanksa.com)

190.34.183.154 (https://metronet.metrobanksa.com).

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

Se informa que aún existen muchas de estas vulnerabilidades como se muestra en la siguiente tabla:

HOST	VULNERABILIDADES	MITIGACIÓN
190.34.183.152	Soporte del protocolo SSL Versión 2 y 3. Suites de Cifrado SSL de seguridad media y baja soportados. Vulnerable a ataques conocidos como **POODLE, BAR MITZVAH**, entre otros.	El protocolo SSL/TLS debe estar configurado para sólo aceptar conexiones de clientes que utilicen la versión TLS 1.2 (esto implica deshabilitar las versiones anteriores como SSL 2, SSL 3, TLS 1.0 y TLS 1.1 y habilitar TLS 1.2) o superior, además solo aceptar suites de cifrado conocidos como no vulnerables.
190.34.183.131	MS15-034: Vulnerabilidad en HTTP.sys puede permitir ejecución de código de manera remota (3042553).	Revisar si este host cuenta con todas las actualizaciones de seguridad recomendadas por Microsoft, en especial, **KB3042553**.

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

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

190.34.183.139	MS15-034: Vulnerabilidad en HTTP.sys puede permitir ejecución de código de manera remota (3042553).	Revisar si este host cuenta con todas las actualizaciones de seguridad recomendadas por Microsoft, en especial, **KB3042553**.
	Soporte del protocolo SSL Versión 2 y 3. Suites de Cifrado SSL de seguridad media y baja soportados. Vulnerable a ataques conocidos como: **POODLE, BAR MITZVAH, FREAK**, entre otros.	El protocolo SSL/TLS debe estar configurado para sólo aceptar conexiones de clientes que utilicen la versión **TLS 1.2** (esto implica deshabilitar las versiones anteriores como SSL 2, SSL 3, TLS 1.0 y TLS 1.1 y habilitar TLS 1.2) o superior, además solo aceptar suites de cifrado conocidos como no vulnerables.
	Protocolo RDP sin restricción de IP de origen (posible **MITM**).	Se debe restringir el acceso a través de **RDP** y sólo permitir direcciones IP origen públicas conocidas y permitidas por

		las políticas de seguridad de su organización para no interrumpir el funcionamiento regular de este host, esto se puede realizar en las reglas avanzadas del **Firewall local de Windows**, Reglas de Firewall que protege a este dispositivo, entre otras.
190.34.183.149	Soporte del protocolo SSL Versión 2 y 3. Suites de Cifrado SSL de seguridad media y baja soportados. Vulnerable a ataques conocidos como **DROWN**, **POODLE**, **BAR MITZVAH**, entre otros.	El protocolo SSL/TLS debe estar configurado para sólo aceptar conexiones de clientes que utilicen la versión **TLS 1.2** (esto implica deshabilitar las versiones anteriores como SSL 2, SSL 3, TLS 1.0 y TLS 1.1 y habilitar TLS 1.2) o superior, además solo aceptar suites de cifrado conocidos como no vulnerables.

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

190.34.183.154	Soporte del protocolo SSL Versión 2 y 3. Suites de Cifrado SSL de seguridad media y baja soportados. Vulnerable a ataques conocidos como **DROWN, POODLE, BAR MITZVAH**, entre otros.	El protocolo SSL/TLS debe estar configurado para sólo aceptar conexiones de clientes que utilicen la versión **TLS 1.2** (esto implica deshabilitar las versiones anteriores como SSL 2, SSL 3, TLS 1.0 y TLS 1.1 y habilitar TLS 1.2) o superior, además solo aceptar suites de cifrado conocidos como no vulnerables.

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

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

Nombre de las reglas las cuales tuvieron más hits en prevención de ataques junto con la cantidad de ocurrencias para cada una registradas por el MSS-APS y MSS-APFW durante el último mes se muestra en la siguiente tabla:

HOST IP	ATAQUES
190.34.183.152	Possible CSRF attack detected in POST (3,213), TCP Scan (vertical) (779), Forbidden Request (481), Parameter Validation Failure (429) y Threat List (277).
190.34.183.131	Possible CSRF attack detected in POST (3,213), TCP Scan (vertical) (779), Forbidden Request (481), Parameter Validation Failure (429) y Threat List (277).

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

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

190.34.183.139	Possible CSRF attack detected in POST (807), Web Scan (581), Threat List (274), Anomaly-SSL-renegotiation-Cli (68) y **block_All_SSLv3_req3** (46).
190.34.183.149	**TCP handshake violation**, first packet not syn (1,310), TCP Scan (vertical) (1,106), **Web Scan** (1,003) , HTTP Page Flood Attack (302) y Threat List (281).
190.34.183.154	HTTP Page Flood Attack (1,138), **TCP handshake violation**, first packet not syn (813), Threat List (278), Possible CSRF attack detected in POST (144) **block_All_SSLv3_req3** (78).

COMENTARIOS Y RECOMENDACIONES

Para las vulnerabilidades de SSL, es recomendable actualizar los servicios para que utilicen TLS 1.2 o 1.3. SSL ya no es considerado un protocolo seguro. TLS es considerado el estándar para las comunicaciones seguras hoy día, sólo en su versión 1.2 y 1.3.

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

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

La vulnerabilidad HTTP.sys Could Allow Remote Code Execution (3042553) es una vulnerabilidad que se debe mitigar con la actualización de seguridad que se considera crítica para todas las ediciones compatibles de Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1 y Windows Server 2012 R2. Se recomienda aplicar parches para Windows 7, 2008 R2, 8, 8.1, 2012 y 2012 R2.

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).