REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

Organización	BANVIVIENDA
Fecha	21/09/2018
Servicio	MSS-EDR
Nivel de Severidad	High
Nivel de Impacto	High
Nivel de Vulnerabilidad	High

DESCRIPCION DE INCIDENTE

Nuestro Centro de Operaciones detectó el intento de **User Brute Force**, en el servidor BpvExch02, host IP 10.100.201.119, el usuario: cynthia.atencio en tres oportunidades reportó 13, 11 y 11 intentos fallidos, respectivamente, desde su red interna a las horas 5:22 pm; 5:5:57 pm y 6:11 pm del presente día.

ACCIONES A TOMAR

Se debe verificar que el usuario que intento iniciar sesión al servidor tenga los permisos y credenciales necesarias para acceder a este host. Verificar host correspondiente a dirección lógica local 10.100.201.113 revisar el "Event Viewer" para información más detallada de este evento.

COMENTARIOS Y RECOMENDACIONES

- Se recomienda implementar una política de bloqueo de cuenta. Después de tres intentos de inicio de sesión fallidos, la cuenta se bloquea hasta que un administrador la desbloquea.
- Otra recomendación es implementar retrasos progresivos. Con esta implementación, las cuentas de los usuarios se bloquean durante un período de tiempo determinado después de algunos intentos fallidos de inicio de sesión.

GLESEC recomienda que se verifique esta información a la brevedad posible.

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).