REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

Organización	BANVIVIENDA
Fecha	24/09/2018
Servicio	MSS-EDR
Nivel de Severidad	Alta
Nivel de Impacto	Alto
Nivel de Vulnerabilidad	Alto

DESCRIPCION DE INCIDENTE

Nuestro servicio MSS-EDR (Endpoint Detection and Response) detectó que los usuarios "banvivienda\cynthia.atencio" y "banvivienda\michelle.harris" intentaron autenticarse varias al servidor "BpvExch02".

El usuario "banvivienda\cynthia.atencio" se intentó autenticar 17 veces, con el último intento registrado a las 12:11 am del 24 de septiembre; y el usuario "banvivienda\michelle.harris" se intentó autenticar 21 veces con el último intento registrado a las 07:37 am del 24 de septiembre. Todos estos intentos de acceso a estas cuentas provienen de la siguiente dirección IP: 10.100.201.113.

COMENTARIOS Y RECOMENDACIONES

Corroborar con los usuarios la actividad de estas cuentas. Estos intentos repetitivos se pueden considerar un ataque de fuerza bruta a dichas cuentas o provenientes de alguna configuración equivocada en alguna aplicación, necesitamos confirmación sobre esta actividad en las cuentas.

Estamos a sus órdenes para apoyarlos con cualquier consulta.

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