

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

Organización	BANVIVIENDA
Fecha	25/09/2018
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 el usuario “banvivienda\dora.rosas” intentaron autenticarse varias veces al servidor “BpvExch02”.

El usuario “banvivienda\dora.rosas” se intentó autenticar 12 veces, con el último intento registrado a las 10:24 am del 25 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.

CONFIDENCIAL



REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

PROTOCOLO DE COMPARTICION DE INFORMACION DE GLESEC

LOS REPORTE DE INCIDENCIAS DE CYBERSEGURIDAD DE GLESEC están en cumplimiento 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).

CONFIDENCIAL

