REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

Organización	BANVIVIENDA
Fecha	11/09/2018
Servicio	MSS-EDR
Nivel de Severidad	High
Nivel de Impacto	High
Nivel de Vulnerabilidad	High

DESCRIPCION DE INCIDENTE

Nuestro centro de Operaciones encontró que diferentes usuarios intentaron autenticarse utilizando NtLmSsp hacia el mismo servidor, este método usa el protocolo NTLM para autenticar usuarios; la manera como este protocolo realiza el proceso de autenticación puede ser aprovechada en ataques como “Pass the Hash” y “SMB relay”. Este evento se produjo desde la dirección IP 10.100.201.113 a BpvExch01 y BpvExch02. Los usuarios encontrados usando este método fueron BANVIVIENDA \milena.batista, BANVIVIENDA \ruthsara.quintero y BANVIVIENDA \agustin.calderon.

ACCIONES A TOMAR

1. Verificar si estos usuarios están autorizados para realizar estas acciones en estos hosts.
2. Corroborar que la autenticación utilizando el protocolo NTLM v1 o NTLM v2 está permitida según sus políticas internas.

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

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBER

COMENTARIOS Y RECOMENDACIONES

Link relevante con respecto a este tema:

- ✓ https://pen-testing.sans.org/blog/2013/04/25/smb-relay-demystified-and-ntlmv2-pwnage-with-python

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

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