INCIDENT REPORT

Organization	BANVIVIENDA
Service	MSS-SIEM
Severity Level	Low
Impact Level	Low
Vulnerability Level	Low

Managed Vulnerability Service (MSS-SIEM)

The MSS-SIEM is an event correlation solution based on GLESEC's Multi-security Appliance ("GMSA") which when connected internally to the network allows sources to receive the data to be correlated and this generates intelligence, alerts and reporting, incident handling and management.

Descripción

En nuestro sistema de monitoreo (GOC), hemos detectado lo siguiente:

La IP 10.100.210.68, tiene una actividad persistente en un periodo corto de tiempo a la IP Interna 10.100.210.1 por el protocolo SNMP.

- La IP 10.100.210.68, ha estado realizando varios intentos de conexión a la IP mencionada.
- Realizando un escaneo a varios puertos conocidos.
- Descubrió que el puerto SNMP, está abierto por lo que intenta conectarse a los siguientes usuarios: lansw, \xA1\xCD\xEE\xF3\xD0\xD4.

Recomendamos verificar el equipo con esa IP y los intentos de accesos.

Adjuntamos imagen de lo mencionado.

i	Event
>	<163>1 2018-04-16T10:17:20-05:00 200.46.19.98 %ASA-3-212006 - - - Dropping SNMP request from 10.100.210.68/21982 to ADMIN:10.100.210.1/snmp because: user not found: lansw
>	<163>1 2018-04-16T10:17:19-05:00 200.46.19.98 %ASA-3-212006 - - - Dropping SNMP request from 10.100.210.68/21982 to ADMIN:10.100.210.1/snmp because: user not found: lansw
>	<163>1 2018-04-16T10:17:17-05:00 200.46.19.98 %ASA-3-212006 - - - Dropping SNMP request from 10.100.210.68/21982 to ADMIN:10.100.210.1/snmp because: user not found: lansw
>	<163>1 2018-04-16T10:17:17-05:00 200.46.19.98 %ASA-3-212006 - - - Dropping SNMP request from 10.100.210.68/21982 to ADMIN:10.100.210.1/snmp because: user not found: \xA1\xCD\xEE\xF3\xD0\xD4
>	<163>1 2018-04-16T10:17:17-05:00 200.46.19.98 %ASA-3-212006 - - - Dropping SNMP request from 10.100.210.68/21726 to ADMIN:10.100.210.1/snmp because: user not found: \xA1\xCD\xEE\xF3\xD0\xD4
>	<163>1 2018-04-16T10:17:17-05:00 200.46.19.98 %ASA-3-212006 - - - Dropping SNMP request from 10.100.210.68/21726 to ADMIN:10.100.210.1/snmp because: user not found: \xA1\xCD\xEE\xF3\xD0\xD4
>	<163>1 2018-04-16T10:17:16-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 10.100.210.68/60852 to ADMIN:10.100.210.1/443
>	<163>1 2018-04-16T10:17:16-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 10.100.210.68/60852 to ADMIN:10.100.210.1/443
>	<163>1 2018-04-16T10:17:15-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 10.100.210.68/60852 to ADMIN:10.100.210.1/443
>	<163>1 2018-04-16T10:17:15-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 10.100.210.68/60843 to ADMIN:10.100.210.1/80
>	<163>1 2018-04-16T10:17:15-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 10.100.210.68/60843 to ADMIN:10.100.210.1/80
>	<163>1 2018-04-16T10:17:14-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 10.100.210.68/60843 to ADMIN:10.100.210.1/80
>	<163>1 2018-04-16T10:17:14-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 10.100.210.68/60840 to ADMIN:10.100.210.1/23
>	<163>1 2018-04-16T10:17:14-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 10.100.210.68/60840 to ADMIN:10.100.210.1/23
>	<163>1 2018-04-16T10:17:13-05:00 200.46.19.98 %ASA-3-710003 - - - TCP access denied by ACL from 10.100.210.68/60840 to ADMIN:10.100.210.1/23

Nota: en caso de ser un comportamiento normal favor notificarnos.

Estamos a sus órdenes para apoyarlos con cualquier consulta.

GLESEC OPERATION CENTER – GOC.