Nombre: Alejandro Asenjo

Objetivo: buscar información de alertas.

Fecha: 21 de julio – 17:19 / Fecha de Verificación 21/07/14 Hora entre 16:30 y 17:13.

Herramientas: logs ubicados en el servidor, y base de snort.

- Open Source Tripwire 2.4 – No presenta errores.
- Iptables – No presenta errores.
- Snort con Base - No presenta ataques relevantes, ni que afecten al sistema.

SNORT

Se localiza un intento de Denegación de Servicio.

< Firma >	< Clasificación >	< Total # >	Sensor #	< Dirección Origen >	< Dirección Dest >	< First >	< Ultimo >
[snort] HTTP: UPS! Y LO SABES...	not-suspicious	235317(91%)	1	14	1	2014-07-09 20:04:28	2014-07-21 17:13:02
[snort] ICMP Destination Unreachable Port Unreachable	misc-activity	5495(2%)	1	4	11	2014-07-09 19:45:21	2014-07-21 17:12:48
[snort] ICMP: ESTAMOS HACIENDO PRUEBAS, Y LO SABES...	not-suspicious	8838(3%)	1	87	11	2014-07-10 17:39:08	2014-07-21 17:12:48
[snort] ICMP Echo Reply	misc-activity	445(0%)	1	77	5	2014-07-09 19:48:23	2014-07-21 17:10:38
[bugtraq] [cve] [icat] [url] [snort] BAD-TRAFFIC same SRC/DST	bad-unknown	229(0%)	1	2	3	2014-07-10 19:59:23	2014-07-21 17:07:30

Se localiza un intento de denegación de servicio por parte de la IP 192.168.32.159.

ID	< Firma >	< Marca de tiempo >	< Dirección Origen >	< Dirección Dest >	< Proto capa 4 >
#0-(1-257838)	[bugtraq] [cve] [icat] [url] [snort] BAD-TRAFFIC same SRC/DST	2014-07-21 17:13:39	192.168.32.159:55951	224.0.0.253:3544	UDP
#1-(1-257623)	[bugtraq] [cve] [icat] [url] [snort] BAD-TRAFFIC same SRC/DST	2014-07-21 17:07:30	192.168.32.159:55951	224.0.0.253:3544	UDP
#2-(1-257491)	[bugtraq] [cve] [icat] [url] [snort] BAD-TRAFFIC same SRC/DST	2014-07-21 17:01:28	192.168.32.159:55951	224.0.0.253:3544	UDP
#3-(1-256938)	[bugtraq] [cve] [icat] [url] [snort] BAD-TRAFFIC same SRC/DST	2014-07-21 16:54:56	192.168.32.159:55951	224.0.0.253:3544	UDP
#4-(1-256662)	[bugtraq] [cve] [icat] [url] [snort] BAD-TRAFFIC same SRC/DST	2014-07-21 16:48:53	192.168.32.159:55951	224.0.0.253:3544	UDP
#5-(1-256609)	[bugtraq] [cve] [icat] [url] [snort] BAD-TRAFFIC same SRC/DST	2014-07-21 16:42:40	192.168.32.159:55951	224.0.0.253:3544	UDP
#6-(1-256574)	[bugtraq] [cve] [icat] [url] [snort] BAD-TRAFFIC same SRC/DST	2014-07-21 16:36:19	192.168.32.159:55951	224.0.0.253:3544	UDP
#7-(1-256564)	[bugtraq] [cve] [icat] [url] [snort] BAD-TRAFFIC same SRC/DST	2014-07-21 16:29:39	192.168.32.159:55951	224.0.0.253:3544	UDP

CVE:

Bugtraq ID:	2666
Class:	Failure to Handle Exceptional Conditions
CVE:	CVE-1999-0016 CVE-2005-0688
Remote:	Yes
Local:	No
Published:	Nov 20 1997 12:00AM
Updated:	Jul 11 2009 06:06AM
Credit:	Posted to BugTraq by m3lt <meltman@lagged.net> on November 20, 1997.

El cual afecta a versiones del kernel Linux kernel 2.0.31 - Linux kernel 2.0.30.