# BOLETÍN DE ALERTA

**Boletín Nro.**: 2017-16
**Fecha de publicación**: 20/11/2017
**Tema**: Vulnerabilidad en ASLR de Windows

**Sistemas afectados**:

- Windows 8, Windows 8.1, y Windows 10

**Descripción**:

Se ha descubierto una vulnerabilidad grave en la implementación de Windows Address Space Layout Randomization (ASLR) en Windows que no activa correctamente dicha protección, dejando los equipos vulnerables a la explotación de otras vulnerabilidades.

ASLR es un mecanismo de protección contra ataques de reutilización de código, incorporado en Windows desde Vista, a través del cual los módulos ejecutables se cargan en direcciones de memoria aleatorias, no predecibles. De esta manera se mitigan los ataques que se basa en código almacenado en direcciones predecibles. Una vulnerabilidad en la implementación de ASLR es el hecho que requiere que el código esté vinculado con el flag /DYNAMICBASE para que utilice ASLR.

Por ello, para proteger a las aplicaciones que no hayan sido compilados con dicho flag, se había incluido una funcionalidad en Microsoft EMET que permite activar mecanismos de protección a nivel del sistema operativo, de forma global y mandatoria para todo el sistema. En las últimas versiones de Windows 10, EMET fue reemplazado por Windows Defender Exploit Guard, que ha incorporado estas funcionalidades.

Antes de Windows 8, la protección global y mandatoria de ASLR se implementaba mediante el registro HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\MoveImages, estableciendo un valor 0xFFFFFFFF en éste. De esta manera, Windows traslada automáticamente el código que tiene una tabla de relocación, de modo a que la ubicación del código en memoria será diferente con cada reinicio y entre diferentes sistemas. Desde Windows 8, la protección global y mandatoria de ASLR se implementa mediante el registro HKLM\System\CurrentControlSet\Control\Session Manager\Kernel\MitigationOptions. Además, es necesario que esté activo el mecanismo de ASRL bottom-up para generar entropía (datos aleatorios) al ASLR.

El problema se da debido a que EMET y Windows Defender Exploit Guard activan ASLR global sin activar también botton-up ASLR global, por lo que no se genera suficiente entropía para iniciar una aplicación en direcciones de memoria aleatorias, lo que en la práctica es equivalente a que ASLR no esté presente. Es decir, por más de que en la interfaz gráfica se selecciona "On by default" o "Activo por defecto", esta



**CERT-PY** Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
**Asunción - Paraguay | www.cert.gov.py**
@CERTpy
/CERT-Py

opción no refleja los valores de los registros subyacentes. Esto genera que el programa es alojado en la misma dirección todas las veces y en otros los sistemas, dejando el sistema expuesto a técnicas de ataques conocidas que se consideraban solucionadas con ASLR.

**Impacto:**

Un cibercriminal puede explotar dicha falla para ejecutar otras técnicas de ataques basadas en reutilización de código. Esta vulnerabilidad, por sí sola, no genera un impacto directo sino debe ser combinada con la explotación de otra vulnerabilidad, del propio sistema operativo o de una aplicación.

**Mitigación:**

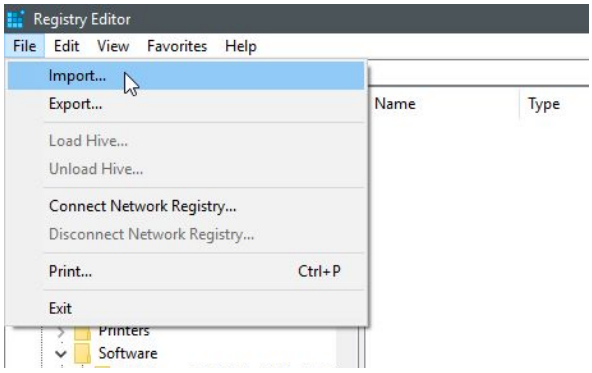
Hasta el momento, no se ha publicado ningún parche para esta vulnerabilidad. Sin embargo, se puede corregir el problema, activando la funcionalidad de ASLR bottom-up y global mandatorio, importando los valores de registro necesarios:

1. Crear un archivo de texto en blanco con el siguiente texto:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\kernel]
"MitigationOptions"=hex:00,01,01,00,00,00,00,00,00,00,00,00,00,00,00,00
```

2. Guardar el archivo con extensión .reg (Ejemplo: ASLR.reg)
3. Abra el Editor de Registros de Windows buscando "regedit" en el Menú de Inicio de Windows
4. Seleccione File > Import .. y seleccione el archivo .reg que acaba de crear.




Note que importar el valor de registro sobreescribirá cualquier mitigación global específica de sistema que esté indicada con dicho registro.

**Información adicional:**
http://www.kb.cert.org/vuls/id/817544

https://www.bleepingcomputer.com/news/security/windows-8-and-later-fail-to-properly-apply-aslr-heres-how-to-fix/



**CERT-PY** Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
**Asunción - Paraguay | www.cert.gov.py**
@CERTpy
/CERT-Py