SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

BOLETÍN DE ALERTA

Boletín Nro.: 2014-07

Fecha de publicación: 15/10/2014

Tema: Vulnerabilidad de Ejecución de Código Remoto en Microsoft Windows OLE Package Manager

Sistemas afectados:

Todas las versiones de Windows desde Windows Vista Service Pack 2 hasta Windows 8.1 y Windows Server version 2008 y 2012.

Descripción:

Una nueva vulnerabilidad critica de ejecución de código remoto en sistemas Windows que afecta a Microsoft Windows OLE Package Manager ha sido publicada el día 14/10/2014, bautizada como “Sandworm”, debido a un grupo de criminales que han estado explotando esta vulnerabilidad en campañas de ciberespionaje.

Esta vulnerabilidad permite a atacantes embeber archivos OLE (*Object Linking and Embebing files*) desde locaciones externas, permitiendo descargar y ejecutar archivos INF. Esto puede ser utilizados para descargar e instalar *malware* en la PC de la victima.

Se han observado campañas de *phishing* distribuyendo archivos PPTX infectados que buscan explotar esta vulnerabilidad para instalar diferentes *Backdoors*, que a su vez permiten la descarga e instalación de otros *malware*. Además incluye un componente para robo de información. Es posible que la vulnerabilidad sea explotada a través de otros tipos de archivo de Office tales como documentos de Word y Excel.

Para este tipo de explotación de la vulnerabilidad es necesaria la interacción de la víctima, ya que es necesario que esta abra el archivo para resultar infectada.

Impacto:

La explotación de la vulnerabilidad permite la ejecución remota de código, siendo posible la descarga, ejecución e instalación de archivos maliciosos.

Solución:
Microsoft publico una actualización que corrige esta vulnerabilidad a través de Microsoft Security Bulletin MS14-060. Se recomienda actualizar los sistemas en la brevedad posible.
Ademas recomendamos no abrir nunca archivos ni adjuntos sospechosos, que sean distribuido tanto en la web como a través de correo electrónico u otros medios.

Información adicional:

https://technet.microsoft.com/library/security/ms14-060
http://www.isightpartners.com/2014/10/cve-2014-4114/
http://www.symantec.com/connect/blogs/sandworm-windows-zero-day-vulnerability-being-actively-exploited-targeted-attacks
http://www.networkworld.com/article/2833485/microsoft-subnet/microsoft-patches-3-zero-days-including-sandworm-on-patch-tuesday.html
https://support.norton.com/sp/es/mx/home/current/solutions/v102743206_EndUserProfile_es_mx
http://nakedsecurity.sophos.com/es/2014/10/15/the-sandworm-malware-what-you-need-to-know/