BOLETÍN DE ALERTA

Boletín Nro.: 2015-07
Fecha de publicación: 23/06/2015
Tema: Vulnerabilidades críticas en Adobe Flash Player

Sistemas afectados:

- Adobe Flash Player 18.0.0.161 y versiones anteriores para Windows y Macintosh
- Adobe Flash Player 11.2.202.466 y versiones anteriores para Linux

Descripción:

Se ha descubierto una nueva vulnerabilidad crítica en Adobe Flash Player, bautizada CVE-2015-3113, que afecta a Windows, Macintosh y Linux, la cual está siendo explotada activamente en campañas de phishing.
El ataque explota una vulnerabilidad en la manera en que Adobe Flash Player parsea archivos de Flash Video (FLV). El exploit utiliza técnicas comunes de corrupción de vector para evadir ASLR (Address Space Layout Randomization), y utiliza programación orientada a retorno (ROP) para eludir la Prevención de ejecución de datos (DEP).
En el empaquetado del exploit se encuentra un código shell junto con la clave para su desencripción. El payload se encuentra codificado mediante XOR y escondido dentro de una imagen .gif.
El exploit está siendo distribuido a través de correos genéricos que aparentan ser spam. En el cuerpo de los correos se encuentran enlaces a servidores comprometidos. Cuando la víctima ingresa al enlace, se ejecuta un script (JavaScript) que en caso de detectar una versión vulnerable de Adobe Flash Player, descarga un archivo Adobe Flash SWF malicioso y un archivo FLV, lo cual infecta al equipo de la víctima, brindando un acceso remoto completo al atacante.
Ésta no es la primera vulnerabilidad crítica descubierta en Adobe Flash Player en los últimos meses, las cuales en su mayoría también pueden ser explotadas para comprometer totalmente el equipo de la víctima.
Se ha observado que, inicialmente, la campaña de phishing va dirigida especialmente a organizaciones de los siguientes sectores: Defensa, Construcción e Ingeniería, Tecnología, Telecomunicaciones, etc.
Adobe ha publicado un parche para la vulnerabilidad.

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

Impacto:
La vulnerabilidad de desbordamiento del búfer de pila puede provocar la ejecución de código remoto por parte de un atacante, permitiendo un control total del equipo infectado.

Solución:
Adobe ha publicado una actualización para todas Adobe Flash Player para Windows, Mac y Linux.

Para determinar la versión de Adobe Flash Player, se puede visitar el siguiente enlace:
http://www.adobe.com/software/flash/about

Para actualizar Adobe Flash Player, visite:
https://get.adobe.com/es/flashplayer/

Recomendación:
Además de mantener Adobe Flash Player, el sistema operativo y todo el software utilizado siempre actualizado, se pueden tomar otras medidas preventivas:

- No abrir nunca archivos adjuntos ni enlaces de correos dudosos, redes sociales, servicios de mensajería u otros. Asegurarse siempre de que la persona que le ha enviado el correo realmente le quería remitir ese adjunto.
- Contar con soluciones de antivirus y mantenerlo actualizado, de modo a prevenir la infección. Si bien en muchos casos se trata de exploits desconocidos, hoy en día la mayoría de las soluciones de seguridad cuentan con mecanismos de protección tempranas.
- Mantener su sistema operativo y el software siempre actualizado, con los últimos parches.
- Evitar la ejecución automática de plugins como Adobe Flash Player, Java, etc. La mayoría de los navegadores modernos permiten configurarlo de modo a que se solicite permiso al usuario cada vez que un sitio web intente ejecutar un plugin. Para ello puede ir a la Configuración o Opciones de su navegador.
    - En Google Chrome, escribir "chrome://settings/content/" en la barra de navegación y en la sección "Complementos", seleccionar “Permitirme decidir cuándo ejecutar contenido de plugins”.
    - En Mozilla Firefox, escribir "about:addons" en la barra de navegación y en cada plugin deseado, seleccionar la opción "Preguntar para activar".

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

- Evitar la ejecución automática de Javascript. Existen complementos como No-Script y ScriptSafe que deshabilitan por defecto la ejecución de Javascript, permitiendo al usuario habilitarlo sólo en las páginas en las que confía.
  https://addons.mozilla.org/es/firefox/addon/noscript/
  https://chrome.google.com/webstore/detail/scriptsafe/oiigbmnaadbkfbmpbfijlflahbdbdgdf

Información adicional:
https://helpx.adobe.com/security/products/flash-player/apsb15-14.html
https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html

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