Muchos de los principales programas actuales han sido pirateados utilizando exploits nuevos y nunca antes vistos, en la edición de este año de la Copa Tianfu, la competencia de hacking más grande y prestigiosa de China.

Celebrada en la ciudad de Chengdu, en el centro de China, la tercera edición de la Copa Tianfu concluyó este domingo.

> *«Se han apuntado muchos objetivos maduros y difíciles en el concurso de este año»,* dijeron los organizadores.

En el evento, se confirmaron exploits exitosos contra:

- iOS 14 ejecutándose en un iPhone 11 Pro
- Samsung Galaxy S20
- Windows 10 v2004 (edición de abril de 2020)
- Ubuntu
- Chrome
- Safari
- Firefox
- Lector PDF de Adobe
- Docker (edición comunitaria)
- VMWare EXSi (hipervisor)
- QEMU (emulador y virtualizador)
- Firmware del enrutador TP-Link y ASUS

15 equipos de hackers chinos participaron en la edición de este año. Los concursantes tenían tres intentos de cinco minutos cada uno para hackear un objetivo seleccionado con un exploit original.

Por cada ataque exitoso, los investigadores recibieron recompensas monetarias que variaron según el objetivo que eligieron y el tipo de vulnerabilidad.

Todas las vulnerabilidades se informaron a los proveedores de software, según las regulaciones del concurso, siguiendo el modelo de las reglas de la competencia de piratería Pwn20wn más establecida que ha tenido lugar en el oeste desde finales de la década del 2000.

Los parches para todos los errores demostrados durante el fin de semana se proporcionarán en los próximos días y semanas, como suele pasar luego de cada concurso de TianfuCup y Pwn20wn.

Al igual que el año pasado, el equipo ganador provino de la compañía china Qihoo 360, nombrado como *«360 Enterprise Security and Government and (ESG) Vulnerability Research Institute»,* el equipo ganador representó casi dos tercios de todo el premio acumulado, y se fueron con $744,500 dólares del total de $1,210,000 otorgados este año.