Los hackers están aprovechando vulnerabilidades conocidas en el software Sunlogin para implementar el marco de comando y control (C2) de Sliver, con el fin de realizar actividades posteriores a la explotación.

Los hallazgos provienen del Centro de Respuesta a Emergencias de Seguridad AhnLab (ASEC), que descubrió que las vulnerabilidades de seguridad en Sunlogin, un programa de escritorio remoto desarrollado en China, están siendo abusadas para implementar una amplia gama de cargas útiles.

> *«Los actores de amenazas no solo usaron la puerta trasera Sliver, sino que también usaron el malware BYOVD (Bring Your Own Vulnerable Driver) para incapacitar los productos de seguridad e instalar shells inversos»,* dijeron los investigadores.

Las cadenas de ataque comienzan con la explotación de dos errores de ejecución remota de código en las versiones de Sunlogin anteriores a la v11.0.0.33 (CNVD-2022-03672 y CNVD-2022-10270), seguido de la entrega de Sliver u otro malware como Gh0st RAT y XMRig crypto.

En uno de los casos, el atacante usó las vulnerabilidades de Sunlogin como arma para instalar un script de PowerShell que, a su vez, emplea la técnica BYOVD para incapacitar el software de seguridad instalado en el sistema y lanzar un shell inverso usando Powercat.

El método BYOVD abusa de un controlador de Windows legítimo pero vulnerable, mhyprot2.sys, que está firmado con un certificado válido para obtener permisos elevados y finalizar los procesos antivirus.

Cabe mencionar que el controlador antitrampas para el videojuego Genshin Impact se usó anteriormente como precursor de la implementación de ransomware, según lo revelado por Trend Micro.

> *«No está confirmado si lo hizo el mismo actor de amenazas, pero después de unas horas, un registro muestra que se instaló una puerta trasera Sliver en el mismo sistema por medio de una explotación de vulnerabilidad Sunlogin RCE»,* dijeron los investigadores.

Los hallazgos se producen cuando los hackers están adoptando Sliver, una herramienta de prueba de penetración legítima basada en Go, como alternativa a Cobalt Strike y Metasploit.

> *«Sliver ofrece las características necesarias paso a paso, como el robo de información de cuenta, el movimiento de la red interna y la superación de la red interna de las empresas, al igual que Cobalt Strike»,* agregaron los investigadores.