REPORTE DE VULNERABILIDAD

LOCAL AUTHENTICATION BYPASS UBUNTU BUDGIE 21.10

26/03/2022

GEORGE-EMILIAN ONOFREI contact@georgeonofrei.com

INTRODUCCIÓN

En este reporte preliminar detallaré el descubrimiento de una vulnerabilidad con impacto potencialmente alto en la que, con acceso local al equipo, permite saltarse la autenticación dentro de un sistema con kernel "Linux budgie 5.13.0-30-generic" y sistema operativo "Ubuntu Budgie 21.10 impish" mediante el uso del cable HDMI.

Una vez conseguido el acceso, podemos ejecutar comandos en la terminal o navegar por los archivos del sistema con los privilegios del último usuario que bloqueó o suspendió el equipo. Desconozco si es posible aplicarlo a otras variantes de Ubuntu u otras versiones de kernel distintas.

METODOLOGÍA

Requisitos:

- **Sistema operativo:** Ubuntu Budgie 21.10 (impish)
- **Versión de kernel:** Linux budgie 5.13.0-30-generic
- **Equipo y configuración:** Un portátil y un monitor externo. El portátil se conecta mediante un cable HDMI al monitor. El monitor está configurado como pantalla principal y en modo extendido o "join displays".

Pasos:

Encendemos el portátil con el cable HDMI conectado al monitor, después, iniciamos sesión con un usuario cualquiera. Una vez tengamos acceso al equipo, lo bloquearemos (también se puede suspender en lugar de bloquear).

Observamos que una vez suspendido o bloqueado, en caso de querer desbloquearlo, nos pedirá la contraseña del usuario nuevamente. Lo que haremos será simplemente desconectar el cable HDMI y automáticamente tendremos acceso al escritorio del usuario sin tener que introducir de nuevo la contraseña.

En caso de que no nos permita utilizar el teclado, bastará con volver a introducir y extraer el cable HDMI para que este funcione de nuevo. También puede haber errores de visualización si iniciamos el navegador u otras aplicaciones, pero nos permite hacer operaciones como ejecutar comandos o navegar y mostrar contenido del explorador de archivos sin ningún problema.

Dejo adjuntado un vídeo mostrando el procedimiento en directo:

https://www.youtube.com/watch?v=cdtbfSj8SUI

Este fallo ha sido reportado por diversos canales al equipo de soporte de Ubuntu Budgie a fecha de 26/03/2022.

Atentamente,
George-Emilian Onofrei