VULNERABILITY REPORT

LOCAL AUTHENTICATION BYPASS UBUNTU BUDGIE 21.10

26/03/2022

GEORGE-EMILIAN ONOFREI contact@georgeonofrei.com

INTRODUCTION

In this preliminary report I will detail the discovery of a vulnerability with potentially high impact in which, with local access to the computer, allows bypassing the authentication inside a system with kernel version "Linux budgie 5.13.0-30-generic" and operating system "Ubuntu Budgie 21.10 impish" by using only the HDMI cable.

Once access is gained, we can run commands in the command terminal or browse the system files with the privileges of the last user who locked or suspended the computer. I don't know if it is possible to apply it to other Ubuntu variants or other different kernel versions.

METODOLOGY

Requirements:

- **Operating system:** Ubuntu Budgie 21.10 (impish)
- **Kernel:** Linux budgie 5.13.0-30-generic
- **Equipment:** A laptop and an external monitor. The laptop is connected via HDMI cable to the monitor. The monitor is configured as the main screen and in "join displays" or "extended" mode.

Steps:

First, we will turn on the laptop and then, we will log in with any user. Once we have logged in, we must lock or suspend the system.

Note that once suspended or locked, if we want to unlock it, it will ask for the user's password again. What we will do is simply disconnect the HDMI cable and we will automatically have access to the user's desktop without having to enter the password again.

In case it does not allow us to use the keyboard, it will be enough to connect and disconnect the HDMI cable for it to work again. There may also be display errors if we start the web browser or other applications, but it will allow us to perform operations such as executing commands or browse and display file explorer content without any problem.

I leave attached a video showing the complete procedure:

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

This security flaw has been reported via multiple channels to the Ubuntu Budgie support team in order to fix it as of 26/03/2022.

Kindly regards,
George-Emilian Onofrei.