TLP:WHITE

# SICK PSIRT
# Security Advisory

## PwnKit vulnerability affects multiple SICK IPCs

Document ID: SCA-2022-0002
Publication Date: 2022-02-23
CVE Identifiers: CVE-2021-4034
Version: V1.0

## SUMMARY

CVE-2021-4034 is a Local Privilege Escalation (LPE) vulnerability, located in the "Polkit" package installed by default on almost every major distribution of the Linux operating system.
On 2022-01-25, Qualys released an advisory for this LPE vulnerability, advising to either update the “Polkit” package or implement the mitigation that Qualys recommends.
In an air-gapped system SICK recommends all customers to implement at least the available mitigation for the corresponding Linux distribution. Please note, that this vulnerability can be exploited only if an user with unprivileged authorization can establish a connection to the systems.

## AFFECTED PRODUCTS*

| **Product** | **Part number / Operating System** | **Remediation available** |
|---|---|---|
| PC, MXE5401, M16G, 1TB, LINUX, CUSTOM | 1111424 / CentOS | Yes |
| PC, MXE5401, M16G, 2TB, C7 | 1099249/ CentOS | Yes |
| PC, MXE5401, M16G, 1TB, C7 | 1099248/ CentO/S | Yes |
| PC, EOS1300, M16G, 1TB, C7 | 1092516/ CentOS | Yes |
| PC, EOS1300, M16G, 2TB, C7 | 1092517/ CentOS | Yes |
| PC, MXE-5401, SSCT, R0, 2TB | 2084896/ RedHat | Yes |
| PC, MXE-5401,R0,2TB,SS-X | 2095232/ RedHat | Yes |
| PC, MXE-5401,R0,2TB,UDS-X | 2104564/ RedHat | Yes |
| PC, MXE-5321, SSXT, R0, 2TB | 2084076/ RedHat | Yes |
| PC, MXE-5321, SSAT, R0, 2TB | 2084077/ RedHat | Yes |
| PC, MXE-5321, UDS, R0, 2TB | 2084078/ RedHat | Yes |
| PC, MXE-5401, SSAT, R0, 2TB | 2084897/ RedHat | Yes |
| PC, MXE-5401, UDS, R0, 2TB | 2084898/ RedHat | Yes |
| PC, MXE-5401, SSCT, R0, 2TB | 2098056/ RedHat | Yes |
| PC, MXE-5401, SP, R0,2TB | 2099100/ RedHat | Yes |
| PC-MXE 5401, CUSTOM, C6, 1TB | 2056761/ CentOS | Yes |
| ERGO,DISP,KIT,C6X,CUSTOM | 2087772/ CentOS | Yes |
| PC, K700-SE-MS4X, M16G, 1TB | 1122338/ UBUNTU | Yes |

*This list is not exhaustive, if you are using a version of Linux Distribution system that was after 2010, you may be impacted.

## VULNERABILITY OVERVIEW

**CVE-2021-4034 Out-of-bounds Write**
The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it'll induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.

**CVE-2021-4034** has been assigned to this vulnerability.
CVSSv3.1 base score: 7.8
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## Mitigations

If no patches are available for your operating system, you can remove the SUID-bit from pkexec as a temporary mitigation using one of the two following ways that is applicable

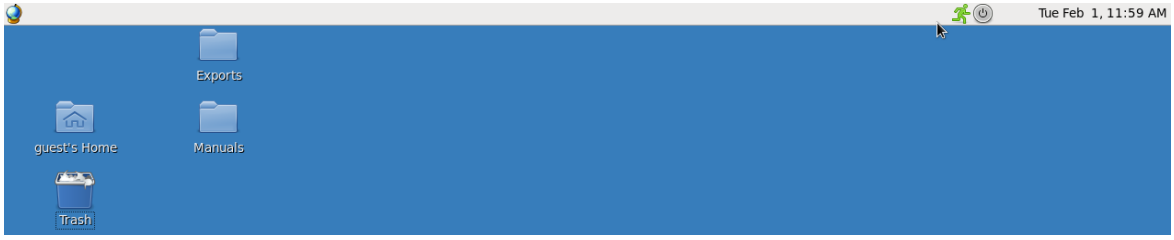
**1. In case your SICK IPC for Analytics has been set up normally, without a "kiosk" mode:**

1. Log in as the <root> user (credentials will be supplied separately).
2. Start the <terminal> app.
3. At the command prompt, enter the following command:
   <chmod 0755 /usr/bin/pkexec>
4. Log out from <root>

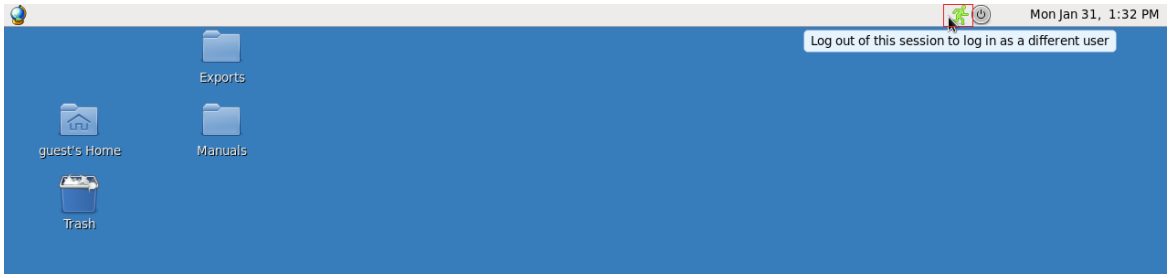
**2. In case your SICK IPC for Analytics has been set up in "kiosk" mode:**

Note: In this below example, the OS is assumed to be CentOS 6.8 running a Gnome 2.28.2 GUI with SICK Package Analytics pre-installed and running on Kiosk mode.

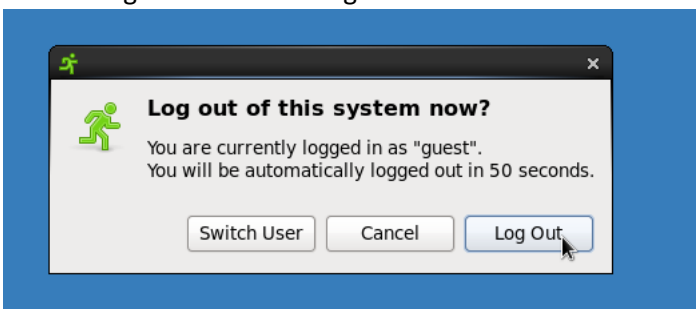
1. These instructions start from the default kiosk-mode display of Package analytics.
2. Press <CTRL+F4> on the keyboard. This will bring up the desktop for the <guest> user.



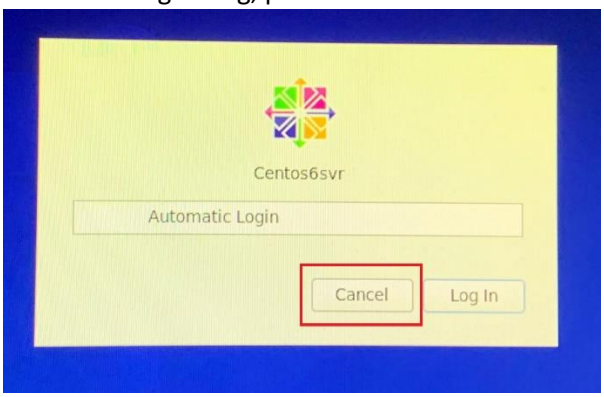

3. Select the green "running man" icon in the upper right.



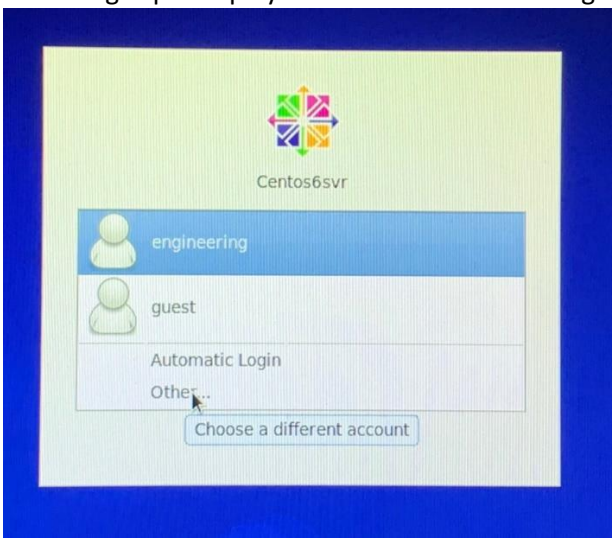
4. Select <Log Out> in the dialog box.



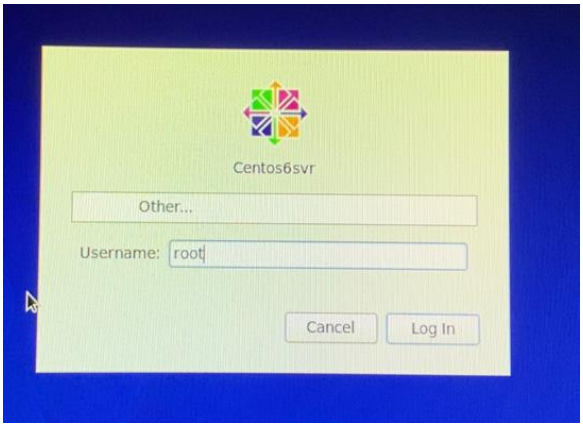

5. In the ensuing dialog, press <Cancel>. It's on a timer, so this step has to be done quickly.



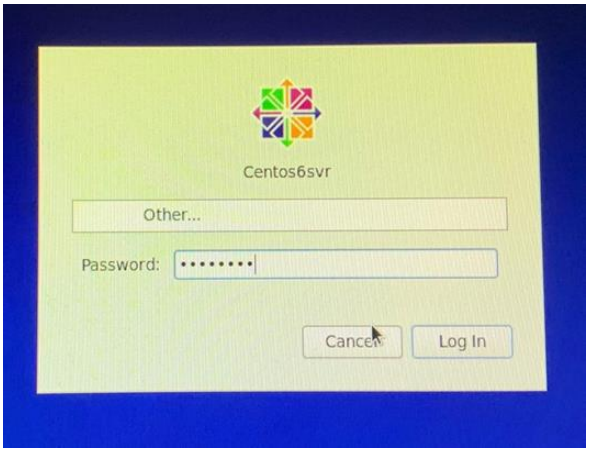

6. This brings up a display that allows the user to log in to other accounts. Select <other>.



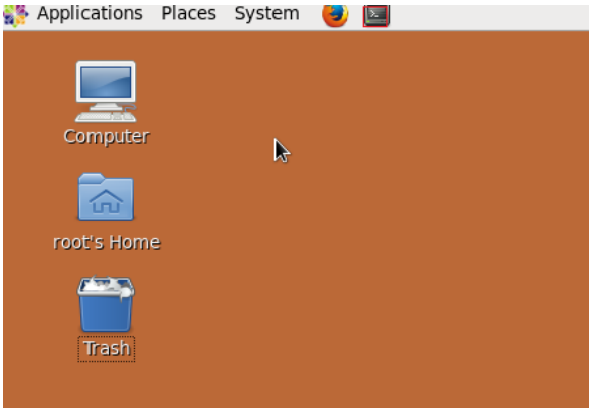
7. Enter <root> as the username.




8. Enter the root password. Note this will be provided in a separate email.

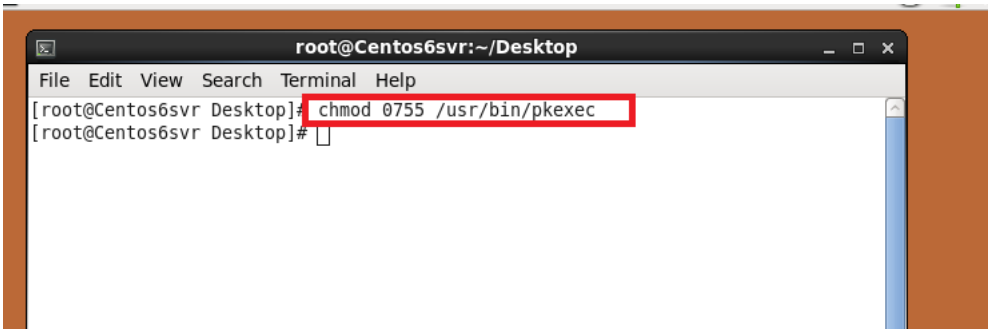



9. This brings up the root desktop. Click on the black terminal icon at the top of the display to bring up the command line prompt.

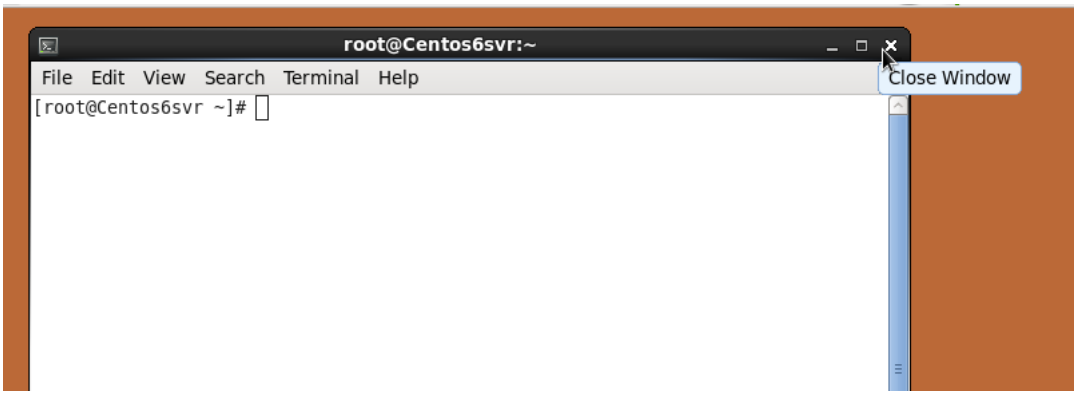


10. At the command line, enter the following command:

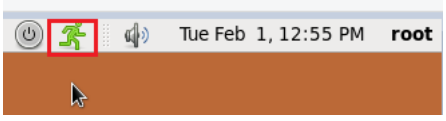
    <chmod 0755 /usr/bin/pkexec>



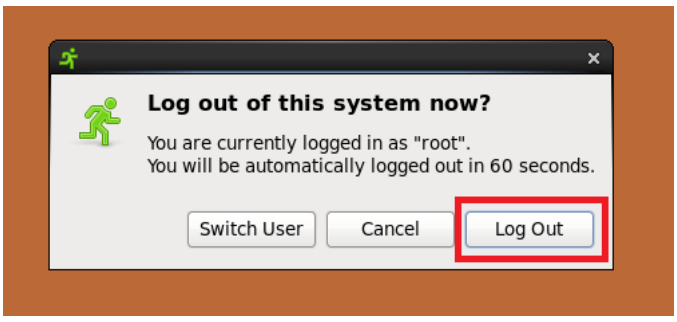

11. Click on the <x> in the upper right to close the terminal window.




12. As before click on the “running man” icon at the top of the display to bring up the logout screen.




13. Select <Log Out> in the ensuing dialogue.



This completes the process. The system will automatically back in as the guest kiosk user.

For Red Hat distributions, the issue can be mitigated by executing the following steps listed on:
https://access.redhat.com/security/vulnerabilities/RHSB-2022-001#mitigation

## GENERAL SECURITY PRACTICES

As general security measures, SICK recommends to minimize network exposure of the devices, restrict network access and follow recommended security practices in order to run the devices in a protected IT environment.

Additional information on Industrial Security can be found at:
http://ics-cert.us-cert.gov/content/recommended-practices

## VULNERABILITY CLASSIFICATION

SICK performs vulnerability classification by using the CVSS scoring system (CVSS v3.x). The environmental score is dependent on the customer's environment and can affect the overall CVSS score. SICK recommends that customers individually evaluate the environmental score to achieve final scoring.

## RESOURCES

SICK PSIRT Security Advisories
https://sick.com/psirt

SICK Operating Guidelines
https://cdn.sick.com/media/docs/1/11/411/Special_information_CYBERSECURITY_BY_SICK_en_IM0084411.PDF

Qualys Advisory
https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt

## HISTORY

| Version | Release Date | Comment |
|---|---|---|
| V1 | 2022-02-23 | Initial Release |