TLP:WHITE

SICK PSIRT
Security Advisory

PwnKit vulnerability affects multiple SICK IPCs

Document ID:	SCA-2022-0002
Publication Date:	2022-02-23
CVE Identifier:	CVE-2021-4034
CVSSv3 Base Score:	7.8
CVSSv3 Vector String:	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Version:	2

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.

List of Products

Product	Part Number	Affected by
SICK ERGO,DISP,KIT,C6X,CUSTOM all versions (CentOS)	2087772	CVE-2021-4034 Status: Fixed Remediation: Vendor fix, Mitigation
SICK PC, EOS1300, M16G, 1TB, C7 all versions (CentOS)	1092516	CVE-2021-4034 Status: Fixed Remediation: Vendor fix, Mitigation

SICK PC, EOS1300, M16G, 2TB, C7 all versions (CentOS)	1092517	CVE-2021-4034 Status: Fixed Remediation: Vendor fix, Mitigation
SICK PC, K700-SE-MS4X, M16G, 1TB all versions (Ubuntu)	1122338	CVE-2021-4034 Status: Fixed Remediation: Vendor fix, Mitigation
SICK PC, MXE-5321, SSAT, R0, 2TB all versions (RedHat)	2084076	CVE-2021-4034 Status: Fixed Remediation: Vendor fix, Mitigation
SICK PC, MXE-5321, SSXT, R0, 2TB all versions (RedHat)	2104564	CVE-2021-4034 Status: Fixed Remediation: Vendor fix, Mitigation
SICK PC, MXE-5321, UDS, R0, 2TB all versions (RedHat)	2084077	CVE-2021-4034 Status: Fixed Remediation: Vendor fix, Mitigation
SICK PC, MXE-5401, SP, R0,2TB all versions (RedHat)	2099100	CVE-2021-4034 Status: Fixed Remediation: Vendor fix, Mitigation
SICK PC, MXE-5401, SSAT, R0, 2TB all versions (RedHat)	2084078	CVE-2021-4034 Status: Fixed Remediation: Vendor fix, Mitigation
SICK PC, MXE-5401, SSCT, R0, 2TB all versions (RedHat)	2084898	CVE-2021-4034 Status: Fixed Remediation: Vendor fix, Mitigation
SICK PC, MXE-5401, UDS, R0, 2TB all versions (RedHat)	2084897	CVE-2021-4034 Status: Fixed Remediation: Vendor fix, Mitigation

SICK PC, MXE-5401,R0,2TB,SS-X all versions (RedHat)	2084896 2098056	CVE-2021-4034 Status: Fixed Remediation: Vendor fix, Mitigation
SICK PC, MXE-5401,R0,2TB,UDS-X all versions (RedHat)	2095232	CVE-2021-4034 Status: Fixed Remediation: Vendor fix, Mitigation
SICK PC, MXE5401, M16G, 1TB, C7 all versions (CentOS)	1099248	CVE-2021-4034 Status: Fixed Remediation: Vendor fix, Mitigation
SICK PC, MXE5401, M16G, 1TB, LINUX, CUSTOM all versions (CentOS)	1111424	CVE-2021-4034 Status: Fixed Remediation: Vendor fix, Mitigation
SICK PC, MXE5401, M16G, 2TB, C7 all versions (CentOS)	1099249	CVE-2021-4034 Status: Fixed Remediation: Vendor fix, Mitigation
SICK PC-MXE 5401, CUSTOM, C6, 1TB all versions (CentOS)	2056761	CVE-2021-4034 Status: Fixed Remediation: Vendor fix, Mitigation

Vulnerability Overview

CVE-2021-4034 Out-of-bounds Write

Description: 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
CWE identifier: CWE-787 (Out-of-bounds Write)

References:

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

Remediations

Vendor Fix for CVE-2021-4034

Details: Update to newest version

Valid for:

- SICK ERGO,DISP,KIT,C6X,CUSTOM all versions (CentOS)
- SICK PC, EOS1300, M16G, 1TB, C7 all versions (CentOS)
- SICK PC, EOS1300, M16G, 2TB, C7 all versions (CentOS)
- SICK PC, K700-SE-MS4X, M16G, 1TB all versions (Ubuntu)
- SICK PC, MXE-5321, SSAT, R0, 2TB all versions (RedHat)
- SICK PC, MXE-5321, SSXT, R0, 2TB all versions (RedHat)
- SICK PC, MXE-5321, UDS, R0, 2TB all versions (RedHat)
- SICK PC, MXE-5401, SP, R0,2TB all versions (RedHat)
- SICK PC, MXE-5401, SSAT, R0, 2TB all versions (RedHat)
- SICK PC, MXE-5401, SSCT, R0, 2TB all versions (RedHat)
- SICK PC, MXE-5401, UDS, R0, 2TB all versions (RedHat)
- SICK PC, MXE-5401,R0,2TB,SS-X all versions (RedHat)
- SICK PC, MXE-5401,R0,2TB,UDS-X all versions (RedHat)
- SICK PC, MXE5401, M16G, 1TB, C7 all versions (CentOS)
- SICK PC, MXE5401, M16G, 1TB, LINUX, CUSTOM all versions (CentOS)
- SICK PC, MXE5401, M16G, 2TB, C7 all versions (CentOS)
- SICK PC-MXE 5401, CUSTOM, C6, 1TB all versions (CentOS)

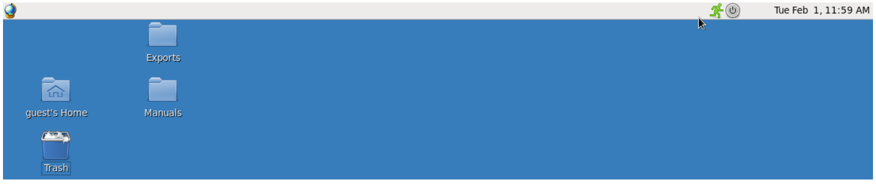
Mitigation for CVE-2021-4034

Details:

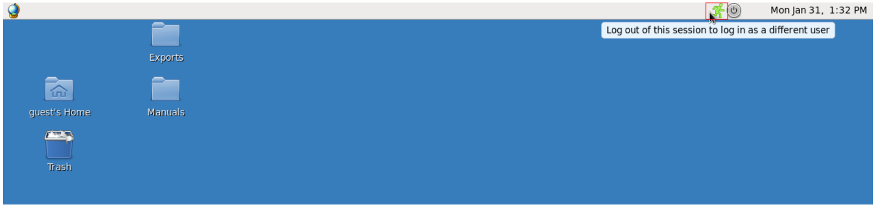
- In case your SICK IPC for Analytics has been set up normally, without a “kiosk” mode:
  - Log in as the <root> user (credentials will be supplied separately).
  - Start the <terminal> app.
  - At the command prompt, enter the following command: <chmod 0755 /usr/bin/pkexec>
  - Log out from <root>
- 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.
  - These instructions start from the default kiosk-mode display of Package analytics.

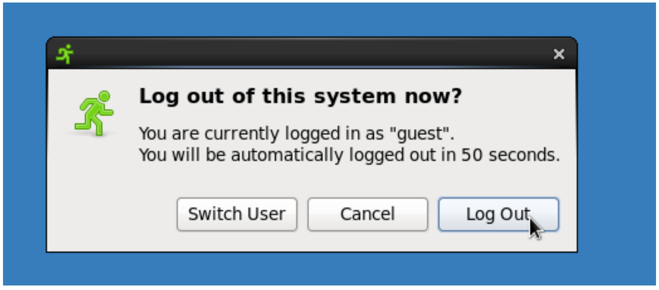
- Press <CTRL+F4> on the keyboard. This will bring up the desktop for the <guest> user.



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



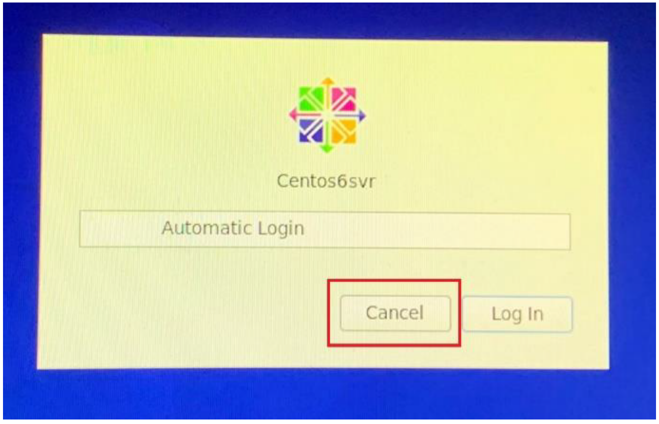
- Select <Log Out> in the dialog box.



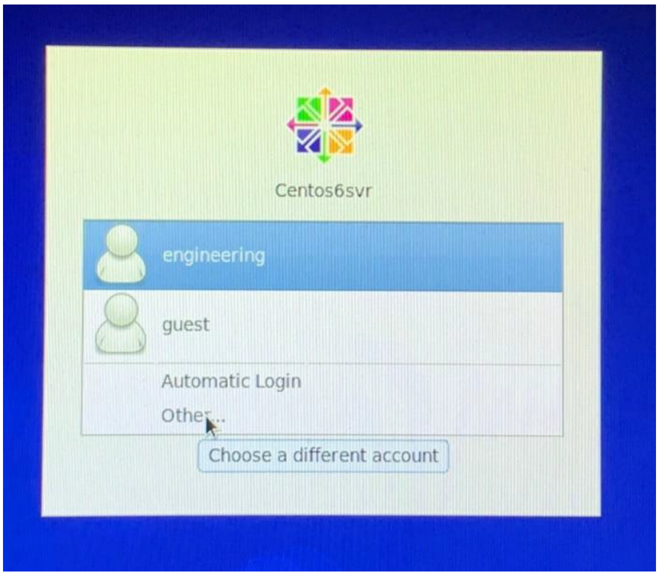
Log out of this system now?

You are currently logged in as "guest".
You will be automatically logged out in 50 seconds.

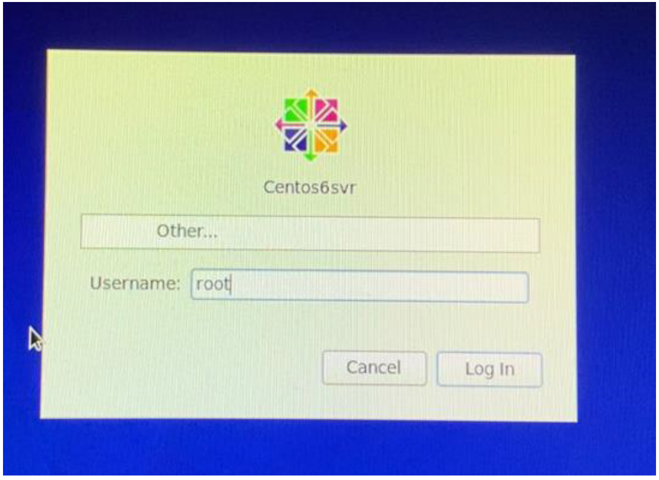
- In the ensuing dialog, press <Cancel>. It's on a timer, so this step has to be done quickly.



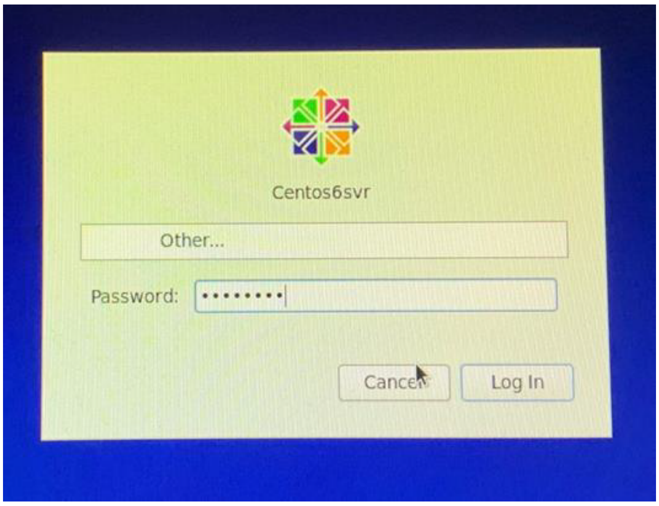
- This brings up a display that allows the user to log in to other accounts. Select <other>.



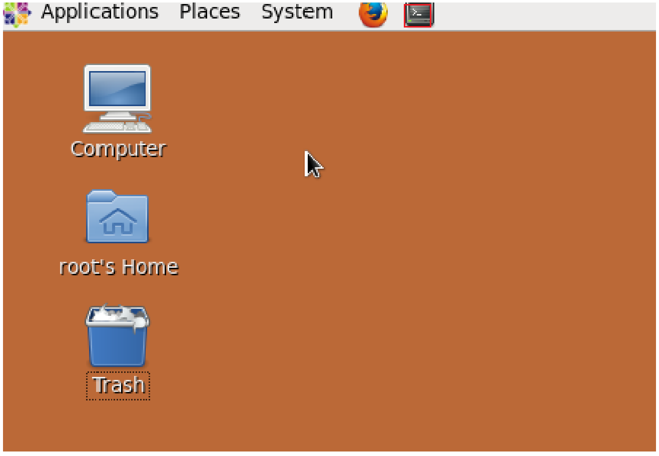
- Enter <root> as the username.



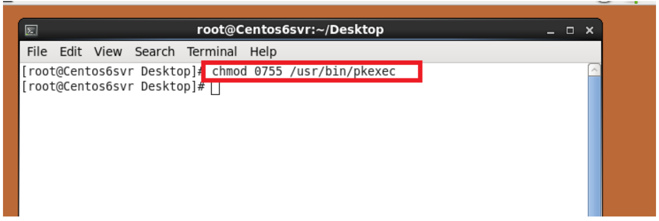
- Enter the root password. Note this will be provided in a separate email.



- 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.

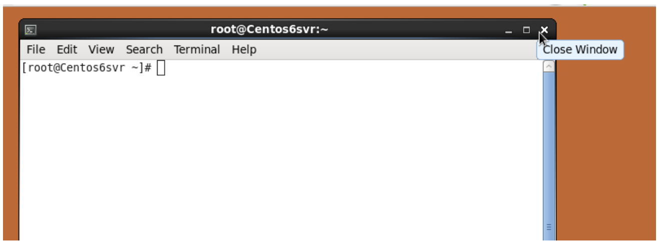


- At the command line, enter the following command: <chmod 0755 /usr/bin/pkexec>



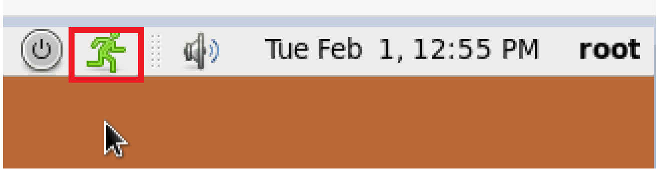
```
[root@Centos6svr Desktop]# chmod 0755 /usr/bin/pkexec
[root@Centos6svr Desktop]# 
```

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

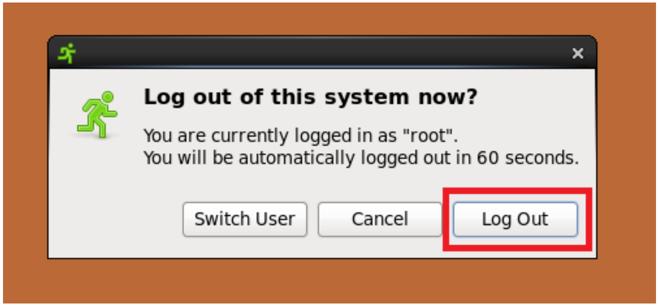


```
[root@Centos6svr ~]#
```

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



– Select <Log Out> in the ensuing dialogue.



Log out of this system now?

You are currently logged in as "root".
You will be automatically logged out in 60 seconds.

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

URL: https://access.redhat.com/security/vulnerabilities/RHSB-2022-001#mitigation

Valid for:

- SICK ERGO,DISP,KIT,C6X,CUSTOM all versions (CentOS)
- SICK PC, EOS1300, M16G, 1TB, C7 all versions (CentOS)
- SICK PC, EOS1300, M16G, 2TB, C7 all versions (CentOS)
- SICK PC, K700-SE-MS4X, M16G, 1TB all versions (Ubuntu)
- SICK PC, MXE-5321, SSAT, R0, 2TB all versions (RedHat)
- SICK PC, MXE-5321, SSXT, R0, 2TB all versions (RedHat)
- SICK PC, MXE-5321, UDS, R0, 2TB all versions (RedHat)
- SICK PC, MXE-5401, SP, R0,2TB all versions (RedHat)
- SICK PC, MXE-5401, SSAT, R0, 2TB all versions (RedHat)
- SICK PC, MXE-5401, SSCT, R0, 2TB all versions (RedHat)
- SICK PC, MXE-5401, UDS, R0, 2TB all versions (RedHat)
- SICK PC, MXE-5401,R0,2TB,SS-X all versions (RedHat)
- SICK PC, MXE-5401,R0,2TB,UDS-X all versions (RedHat)

- SICK PC, MXE5401, M16G, 1TB, C7 all versions (CentOS)
- SICK PC, MXE5401, M16G, 1TB, LINUX, CUSTOM all versions (CentOS)
- SICK PC, MXE5401, M16G, 2TB, C7 all versions (CentOS)
- SICK PC-MXE 5401, CUSTOM, C6, 1TB all versions (CentOS)

General Security Practices

General Security Measures

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.

Vulnerability Classification

SICK performs vulnerability classification by using the CVSS scoring system (*CVSS v3.1*). 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

ICS-CERT recommended practices on Industrial Security:
http://ics-cert.us-cert.gov/content/recommended-practices

CVSS v3.1 Calculator:
https://www.first.org/cvss/calculator/3.1

History

Version	Release Date	Comment
1	2022-02-23	Initial release
2	2023-02-10	Updated Advisory (only visual changes)