The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

https://www.cisa.gov/tlp

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:

01/26/2022

SUBJECT:

A Vulnerability in Polkit's pkexec Component Could Allow For Local Privilege Escalation

OVERVIEW:

A vulnerability in Polkit's pkexec component could allow for local privilege escalation. Polkit (formerly PolicyKit) is a component for controlling system-wide privileges in Unix-like operating systems. It provides an organized way for non-privileged processes to communicate with privileged ones. Polkit is installed by default on all major Linux distributions. Successful exploitation of this vulnerability could result in privilege escalation to root privileges.

THREAT INTELLIGENCE:

Qualys and Bleeping Computer have mentioned this vulnerability is extremely easy to exploit. Bleeping Computer has confirmed exploitation code has been released to the public.

SYSTEMS AFFECTED:

- All Linux systems with the policykit package installed
- Ubuntu versions 14.04, 16.04, 18.04, 20.04, 21.10
- Debian Distributions
- Fedora Distributions
- CentOS Distributions
- Red Hat Enterprise Linux 6 Extended Lifecycle Support
- Red Hat Enterprise Linux 7
- Red Hat Enterprise Linux 7.3 Advanced Update Support
- Red Hat Enterprise Linux 7.4 Advanced Update Support
- Red Hat Enterprise Linux 7.6 Advanced Update Support
- Red Hat Enterprise Linux 7.6 Telco Extended Update Support
- Red Hat Enterprise Linux 7.6 Update Services for SAP Solutions
- Red Hat Enterprise Linux 7.7 Advanced Update Support
- Red Hat Enterprise Linux 7.7 Telco Extended Update Support
- Red Hat Enterprise Linux 7.7 Update Services for SAP Solutions
- Red Hat Enterprise Linux 8
- Red Hat Enterprise Linux 8.1 Update Services for SAP Solutions
- Red Hat Enterprise Linux 8.2 Extended Update Support
- Red Hat Enterprise Linux 8.4 Extended Update Support

RISK:
Government:
- Large and medium government entities: **Medium**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **Medium**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability in Polkit 's pkexec component could allow for local privilege escalation. The current version of pkexec doesn't handle the calling parameters count correctly and ends up 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. Successful exploitation of this vulnerability could result in privilege escalation to root privileges.

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate patches to vulnerable systems immediately after appropriate testing.
- If a patch is not available for your distribution of Linux, you can remove the SUID-bit from pkexec as a temporary mitigation: chmod 0755 /usr/bin/pkexec
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:
CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4034

Qualys:
https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034

Bleeping Computer:
https://www.bleepingcomputer.com/news/security/linux-system-service-bug-gives-root-on-all-major-distros-exploit-released/

Redhat:
https://access.redhat.com/security/cve/CVE-2021-4034

Ubuntu:
https://ubuntu.com/security/notices/USN-5252-2
https://ubuntu.com/security/notices/USN-5252-1

Debian:
https://security-tracker.debian.org/tracker/CVE-2021-4034

TLP: WHITE

https://www.cisa.gov/tlp

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.