Report on

PWNKITCVE-2021-4034

CVE-2021-41773/42013

BY

Arsalan AKmal

PwnKit (CVE-2021-4034)

PwnKit (CVE-2021-4034) is a critical privilege escalation vulnerability found in the `pkexec` utility of the `polkit` package, which is widely used on Linux systems. The vulnerability was discovered by security researchers from Qualys in late 2021 and affects all major Linux distributions.

Understanding `pkexec` and `polkit`

- **`pkexec`**: This is a command-line tool that is part of `polkit` (formerly known as PolicyKit). It allows an authorized user to execute commands as another user, typically root. The `pkexec` command is similar to `sudo` but is designed to be used in graphical desktop environments to handle privilege escalation in a more secure and standardized manner.
- **`polkit`**: A toolkit for defining and handling authorizations, `polkit` is used by many Linux distributions to manage permissions for various administrative tasks.

What is CVE-2021-4034 (PwnKit)?

CVE-2021-4034, dubbed "PwnKit," is a local privilege escalation vulnerability in the `pkexec` utility. The vulnerability is caused by an uninitialized memory problem in the `pkexec` utility. This flaw allows a local unprivileged user to escalate their privileges to root.

How the Vulnerability Works

1. **Uninitialized Memory Read**: The vulnerability is due to an uninitialized memory read in the `pkexec` program. When `pkexec` is executed without any arguments, it does not properly initialize certain memory locations before using them.
2. **Manipulating Environment Variables**: By manipulating the environment variables, an attacker can control the execution flow of the `pkexec` program, leading to arbitrary code execution as the root user.
3. **Local Exploitation**: The attacker must have local access to the system, but once they exploit the vulnerability, they can gain root-level privileges, which could allow them to perform any action on the compromised system.

Impact of the Vulnerability

- **Privilege Escalation**: PwnKit is a local privilege escalation vulnerability, meaning it allows an attacker who already has limited access to a Linux system to elevate their privileges to root, gaining full control over the system.
- **Widespread Impact**: Since `polkit` is installed by default on many Linux distributions (such as Ubuntu, Debian, Fedora, Red Hat, and others), a large number of systems are potentially vulnerable.

Mitigation and Patching

- **Patches Released**: Once the vulnerability was publicly disclosed, most major Linux distributions released patches to fix the issue in the `polkit` package.
- **Update Your System**: To protect against this vulnerability, you should update your system's packages to the latest versions using your distribution's package manager. For example:
    - On Debian/Ubuntu systems:

      ```
      bash
      Copy code
      sudo apt update && sudo apt upgrade
      ```

    - On Red Hat/Fedora systems:

      ```
      bash
      Copy code
      sudo dnf update
      ```

- **Temporary Workaround**: Before patches were available, a common workaround was to remove the `setuid` bit from `pkexec`, although this would disable its functionality:

  ```
  bash
  Copy code
  chmod 0755 /usr/bin/pkexec
  ```

Summary

PwnKit (CVE-2021-4034) is a critical local privilege escalation vulnerability in the `pkexec` utility of `polkit`, affecting many Linux distributions. It allows a local attacker to gain root privileges due to improper handling of environment variables and uninitialized memory. The vulnerability was patched by Linux distributions shortly after its discovery, and it is essential to update affected systems to mitigate the risk.

CVE-2021-41773 and **CVE-2021-42013**

CVE-2021-41773 and **CVE-2021-42013** are two related security vulnerabilities in the Apache HTTP Server (often referred to as Apache or httpd). These vulnerabilities are both **path traversal** and **remote code execution (RCE)** issues, affecting certain versions of the Apache web server.

CVE-2021-41773: Path Traversal and File Disclosure

CVE-2021-41773 is a path traversal vulnerability in the Apache HTTP Server 2.4.49.

Key Details:

1. **Path Traversal Vulnerability**: The vulnerability allows an attacker to use specially crafted URLs to gain access to files outside the document root of the web server. This is done by bypassing path checks using encoded characters in the URL, such as `%2e` for `.` (dot).
2. **File Disclosure**: If files outside the document root are accessible (i.e., not protected by restrictive permissions), an attacker can read them. This could include sensitive files like `/etc/passwd` on Linux systems.
3. **Affected Versions**: Apache HTTP Server 2.4.49 is the main affected version. This vulnerability occurs because the URL normalization process does not correctly handle encoded path traversal sequences.
4. **Patch and Mitigation**: Apache quickly released version 2.4.50 to fix this issue by correctly validating and normalizing the path in requests.

CVE-2021-42013: Path Traversal and Remote Code Execution (RCE)

CVE-2021-42013 is a follow-up vulnerability found in Apache HTTP Server 2.4.50, the initial patch release for CVE-2021-41773.

Key Details:

1. **Incomplete Fix for CVE-2021-41773**: The fix in Apache HTTP Server 2.4.50 did not adequately resolve the path traversal issue. Attackers could still use similar techniques to access files outside the document root.
2. **Remote Code Execution (RCE)**: If the Apache server is configured to allow CGI script execution (e.g., through the `mod_cgi` module) and certain permissions are not restrictive, attackers could execute arbitrary code on the server. This makes the vulnerability significantly more dangerous because it enables not just file disclosure but also remote code execution.
3. **Affected Versions**: Apache HTTP Server 2.4.50 is primarily affected. The vulnerability allows attackers to bypass security restrictions intended to prevent access to certain files and directories.
4. **Patch and Mitigation**: Apache released version 2.4.51 to fully address both CVE-2021-41773 and CVE-2021-42013. This update ensures proper path normalization and checks to prevent path traversal and RCE vulnerabilities.

Summary of the Vulnerabilities

- **CVE-2021-41773**: Path traversal vulnerability in Apache HTTP Server 2.4.49 that allows file disclosure.
- **CVE-2021-42013**: Path traversal and RCE vulnerability in Apache HTTP Server 2.4.50 due to incomplete fixes for CVE-2021-41773.

Mitigation and Recommendations

1. **Upgrade to Latest Version**: Ensure that your Apache HTTP Server is updated to version 2.4.51 or later. This version includes the complete patches for both vulnerabilities.

   ```
   bash
   Copy code
   # Example command for Ubuntu/Debian-based systems
   sudo apt update && sudo apt install apache2

   # Example command for Red Hat/CentOS-based systems
   sudo yum update httpd
   ```

2. **Restrict Directory and File Permissions**: Ensure that sensitive files are not accessible to the Apache process and configure appropriate file permissions.
3. **Disable CGI Execution if Unnecessary**: If your web application does not require CGI execution, disable it to reduce the risk of RCE vulnerabilities.
4. **Monitor and Audit Logs**: Regularly monitor and audit server logs for any unusual access patterns or attempts to exploit path traversal vulnerabilities.

By taking these steps, you can help protect your Apache server from these vulnerabilities and maintain a secure web environment.