Linux 資訊安全檢測與漏洞分析

作者：U10916024張呈顥
指導教授：盧東華 助理教授

Binary Exploitation
PWN

武田奈々

I. 堆疊
The Stack

II. 緩衝區溢位
Buffer Overflow

III. 記憶體洩漏
Memory Leak

CVE-2021-4034
PKEXEC

武田奈々

POLKIT之PKEXEC指令可進行提權

POLKIT簡介

polkit 是一個在Unix like 作業系統中，用來控制系統process權限的一套工具

- 非特權行程以一個有系統性的方式與特權行程進行溝通
- 使用polkit裡面具有提升權限的指令pkexec，來取得root權限
- polkit並沒有賦予完全的root權限

pkexec簡介

Qualys 形容此漏洞是攻擊者的美夢成真：

- pkexec被預設安裝在Linux的各個發行版上
- 此漏洞自2009年5月就存在了
  - commit c8c3d83, “Add a pkexec(1) command”
- 任何非特權使用者都可以取得完整的root權限
- 就算polkit本身沒有運作，此漏洞也可以被利用

Linux版本

```
Program version:                3.0.8
Operating system:               Linux
Operating system name:          CentOS Linux
Operating system version:       7
Kernel version:                 3.10.0
Hardware platform:              x86_64
```

pkexec版本

```
[takeda@localhost ~]$ pkexec --version
pkexec version 0.112
```

BEFORE

```
[takeda@localhost ~]$ id
uid=1883(takeda) gid=1884(takeda) groups=1884(takeda),10(wheel)
```

AFTER

```
[takeda@localhost polkit-pkexec-ex]$ ./exploit
Current User before execute exploit
hacker@victim$whoami: takeda
Exploit written by @luijait (0x6c75696a616974)
[+] Enjoy your root if exploit was completed succesfully
[root@localhost polkit-pkexec-ex]# id
uid=0(root) gid=0(root) groups=0(root),10(wheel),1884(takeda)
[root@localhost polkit-pkexec-ex]#
```

Analysis

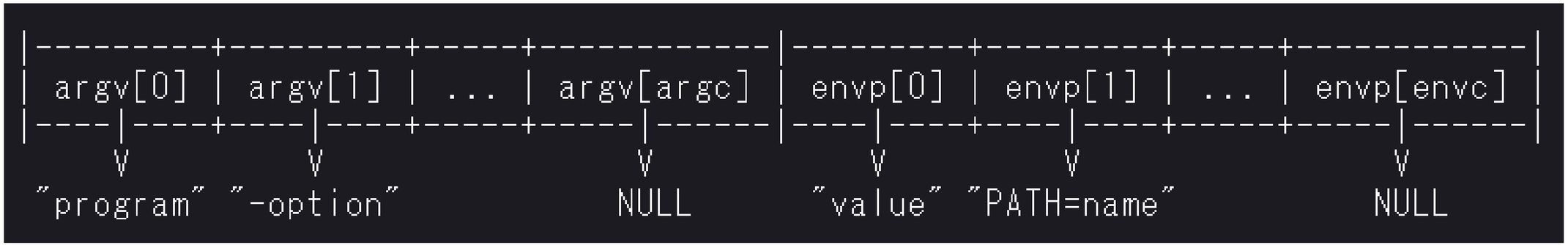
```
435 main (int argc, char *argv[])
436 {
...
534   for (n = 1; n < (guint) argc; n++)
535     {
...
568     }
...
610   path = g_strdup (argv[n]);
...
629   if (path[0] != '/')
630     {
...
632       s = g_find_program_in_path (path);
...
639       argv[n] = path = s;
640     }
```

Analysis

```
435 main (int argc, char *argv[])
436 {
...
534   for (n = 1; n < (guint) argc; n++)
535     {
...
568     }
...
610   path = g_strdup (argv[n]);
...
629   if (path[0] != '/')
630     {
...
632       s = g_find_program_in_path (path);
...
639       argv[n] = path = s;
640     }
```

Unfortunately, if the number of command-line arguments argc is 0 (if the argument list argv that we pass to execve() is empty, i.e. {NULL}), then argv[0] is NULL.
(the argument list's terminator)

環境變數之記憶體配置


argv[0]
argv[1]
...
argv[argc]
envp[0]
envp[1]
...
envp[envc]
"program"
"-option"
NULL
"value"
"PATH=name"
NULL

Analysis

```
435 main (int argc, char *argv[])
436 {
...
534   for (n = 1; n < (guint) argc; n++)
535     {
...
568     }
...
610   path = g_strdup (argv[n]);
...
629   if (path[0] != '/')
630     {
...
632       s = g_find_program_in_path (path);
...
639       argv[n] = path = s;
640     }
```

Analysis

```
435 main (int argc, char *argv[])
436 {
...
534   for (n = 1; n < (guint) argc; n++)
535     {
...
568     }
...
610   path = g_strdup (argv[n]);
...
629   if (path[0] != '/')
630     {
...
632       s = g_find_program_in_path (path);
...
639       argv[n] = path = s;
640     }
```

文獻探討

武田奈々

參照

[1] Qualys, “pwnkit.txt,” 25 1 2022. [線上]. Available: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt.

[2] C. Walters, “pkexe.c,” 5 7 2015. [線上]. Available: https://gitlab.freedesktop.org/polkit/polkit/-/blob/0.120/src/programs/pkexec.c.

[3] J. Bharat, “PwnKit: Local Privilege Escalation Vulnerability Discovered in polkit’s pkexec (CVE-2021-4034),” Qualys, 25 1 2022. [線上]. Available: https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-local-privilege-escalation-vulnerability-discovered-in-polkits-pkexec-cve-2021-4034.

[4] H. Red, “RHSB-2022-001 Polkit Privilege Escalation - (CVE-2021-4034),” 25 1 2022. [線上]. Available: https://access.redhat.com/security/vulnerabilities/RHSB-2022-001.

[5] 360 冰刃实验室, “CVE-2021-4034 pkexec 本地提权漏洞利用解析,” 安全客, 14 2 2022. [線上]. Available: https://www.anquanke.com/post/id/267774#h3-5.

[6] 万海旭, “CVE-2021-4034 polkit（pkexec）提权漏洞复现,” 腾讯云, 22 2 2022. [線上]. Available: https://cloud.tencent.com/developer/article/1945253.

THANK YOU

Have any questions?

wind.ware1203@gmail.com

武田奈々