BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 32 /TTCNTT-KTHT
V/v lỗ hổng bảo mật CVE-2021-4034 trong Polkit pkexec ảnh hưởng nghiêm trọng đến hệ điều hành Linux

Hà Nội, ngày 09 tháng 02 năm 2022

Kính gửi: Các đơn vị trực thuộc Bộ có hệ thống thông tin

Ngày 25/01/2022, các nhà nghiên cứu bảo mật đã công bố thông tin cảnh báo về lỗ hổng bảo mật CVE-2021-4034 (hay còn gọi là PwnKit) trong thành phần pkexec của Polkit ảnh hưởng nghiêm trọng đến hệ điều hành Linux, cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền với một tài khoản người dùng bất kỳ trong hệ thống mục tiêu.

Polkit là một thành phần mặc định của nhiều bản phân phối Linux được dùng để kiểm soát và quản lý các đặc quyền trong hệ thống. Lỗ hổng này có mức ảnh hưởng khá lớn do hệ điều hành Linux đang được sử dụng khá phổ biến trong nhiều hệ thống thông tin của cơ quan, tổ chức hiện nay. Hiện tại đã có mã khai thác được công bố rộng rãi trên Internet.

Thông tin chi tiết lỗ hổng bảo mật có tại Phụ lục kèm theo.

Nhằm bảo đảm an toàn thông tin cho hệ thống thông tin của Quý đơn vị, Trung tâm Công nghệ thông tin khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát, xác định các hệ thống thông tin sử dụng hệ điều hành Linux có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công trong trường hợp chưa thể cập nhật bản vá cần thực hiện các bước khắc phục thay thế để giảm thiểu nguy cơ bị tấn công (tham khảo thông tin tại Phụ lục kèm theo).

2. Rà soát, giám sát các dấu hiệu liên quan đến các hành vi khai thác lỗ hổng này trên toàn bộ hệ thống thông tin để phát hiện và xử lý kịp thời các dấu hiệu tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

3. Báo cáo kết quả xử lý lỗ hổng nêu trên về Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, thư điện tử: phongktht@most.gov.vn **trước ngày 23/2/2022**.

Trong trường hợp cần thiết, Quý đơn vị liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, điện thoại 024.39439060, thư điện tử: phongktht@most.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Cổng thông tin điện tử Bộ KH&CN;
- Lưu: VT, KTHT.

GIÁM ĐỐC

BỘ KHOA HỌC CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

Phụ lục
Thông tin về các lỗ hổng bảo mật CVE-2021-4034
(Kèm theo Công văn số 32 /TTCNTT-KTHT ngày 09 /02 /2022 của Trung tâm Công nghệ thông tin)

1. Thông tin lỗ hổng bảo mật

- CVSS: 7.8 (cao)

- Mô tả: Lỗ hổng tồn tại trong pkexec của polkit, cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền với một tài khoản người dùng bất kỳ.

- Ảnh hưởng: Red Hat Enterprise Linux 6/7/8, Red Hat Virtualization 4, các cấu hình mặc định trên Ubuntu, Debian, Fedora và CentOS,….

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho lỗ hổng bảo mật nói trên. Tuy nhiên trong trường hợp chưa thể cập nhật, Quý đơn vị có thể thực hiện các bước khắc phục thay thế như sau:

Đối với hệ điều hành Red Hat

Bước 1: Cài đặt required systemtap packages và dependencies

https://access.redhat.com/solutions/5441.

Bước 2: Cài đặt thông tin gỡ lỗi polkit

```
debuginfo-install polkit
```

Bước 3: Tạo script systemtap và đặt tên là pkexec-block.stp

```
probe process("/usr/bin/pkexec").function("main") {
if (cmdline_arg(1) == "")
raise(9);
}
```

Bước 4: Tải systemtap module vào kernel đang chạy

```
stap -g -F -m stap_pkexec_block pkexec_block.stp
```

Bước 5: Kiểm tra đảm bảo module đã được tải vào kernel

```
lsmod | grep -i stap_pkexec_block
stap_pkexec_block 434176 0
```

Bước 6: Sau khi polkit package đã được cập nhật lên phiên bản đã có chứa bản vá, systemtap generated kernel module có thể xóa bằng cách chạy

```
rmmod stap_pkexec_block
```

Lưu ý: Các bước giảm thiểu này không được áp dụng đối với hệ thống có sử

dụng Secure Boot.

Đối với các bản phân phối Linux khác

Có thể thực hiện bằng cách bỏ quyền suid với /usr/bin/pkexec bằng cách thực hiện câu lệnh sau với quyền root

```
chmod 0755 /usr/bin/pkexec
```

Hoặc

```
chmod u-s /usr/bin/pkexec
```

Lưu ý: Việc này có thể khiến cho hệ điều hành có thể hoạt động không như mong muốn.

3. Tài liệu tham khảo

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

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

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số 32 /TTCNTT-KTHT ngày09 /02 /2022 của Trung tâm Công nghệ thông tin)

TT	Tên đơn vị
1.	Thanh tra Bộ
2.	Cục Công tác phía Nam
3.	Cục Ứng dụng và phát triển công nghệ
4.	Cục Năng lượng nguyên tử
5.	Cục Thông tin Khoa học và Công nghệ Quốc gia
6.	Cục Phát triển thị trường và doanh nghiệp khoa học và công nghệ
7.	Cục An toàn bức xạ và hạt nhân
8.	Cục Sở hữu trí tuệ
9.	Tổng Cục tiêu chuẩn đo lường chất lượng
10.	Ban quản lý khu công nghệ cao Hoà Lạc
11.	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
12.	Viện Khoa học và công nghệ Việt Nam - Hàn Quốc (VKIST)
13.	Viện Nghiên cứu sáng chế và Khai thác công nghệ
14.	Viện Năng lượng nguyên tử Việt Nam
15.	Viện Ứng dụng công nghệ
16.	Viện Đánh giá khoa học và Định giá công nghệ
17.	Viện Khoa học sở hữu trí tuệ
18.	Viện Nghiên cứu và Phát triển Vùng
19.	Văn phòng các Chương trình trọng điểm cấp nhà nước
20.	Văn phòng Công nhận chất lượng
21.	Văn phòng Đăng ký hoạt động khoa học và công nghệ
22.	Văn phòng các Chương trình khoa học và công nghệ quốc gia
23.	Báo Khoa học và Phát triển
24.	Tạp chí Khoa học và Công nghệ Việt Nam
25.	Nhà xuất bản Khoa học và Kỹ thuật
26.	Quỹ Phát triển khoa học và công nghệ quốc gia
27.	Quỹ Đổi mới công nghệ quốc gia
28.	Trung tâm Nghiên cứu và Phát triển truyền thông khoa học và công nghệ
29.	Trung tâm Nghiên cứu và Phát triển hội nhập khoa học và công nghệ quốc tế