BỘ THÔNG TIN TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

Số: 144 /CATTT-NCSC
V/v lỗ hổng bảo mật CVE-2021-4034 trong Polkit pkexec ảnh hưởng nghiêm trọng đến hệ điều hành Linux

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

Hà Nội, ngày 27 tháng 01 năm 2022

Kính gửi:

- Đơn vị chuyên trách về CNTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; các Ngân hàng TMCP; các tổ chức tài chính;
- Hệ thống các đơn vị chuyên trách về an toàn 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 đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Cục An toàn 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 Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), thư điện tử: ais@mic.gov.vn trước ngày 25/2/2021.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng (để b/c);
- Cục A05, Bộ Công an;
- Bộ Tư lệnh 86, Bộ Quốc phòng;
- Ban Cơ yếu Chính phủ;
- Cục trưởng;
- Trung tâm VNCERT/CC, phòng ATHTTT;
- Lưu: VT, NCSC.

CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Thành Phúc

Phụ lục

THÔNG TIN VỀ LỖ HỔNG BẢO MẬT CVE-2021-4034

(Kèm theo Công văn số /CATTT-NCSC ngày / /2022 của Cục An toàn 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