BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

Số: 106 /CNTT-YTĐT
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 18 *tháng* 02 *năm 2022*

Kính gửi:

- Vụ, Cục, Tổng cục, Văn phòng Bộ, Thanh tra Bộ;
- Các đơn vị trực thuộc Bộ Y tế;
- Các Sở Y tế.

Cục Công nghệ thông tin nhận được công văn 144 /CATTT-NCSC ngày 27/01/2022 của Cục An toàn thông tin về lỗ hổng bảo mật CVE-2021-4034 trong Polkit pkexec ảnh hưởng nghiêm trọng đến hệ điều hành Linux.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, Cục Công nghệ thông tin trân trọng đề nghị Quý đơn vị:

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.

Trong trường hợp cần thiết, Quý Đơn vị liên hệ Trung tâm Dữ liệu y tế, Cục Công nghệ thông tin, Bộ Y tế (ThS. Hoàng Đăng Trị, điện thoại: 0987772483; Email: trihd.cntt@moh.gov.vn) để được hỗ trợ.

Trân trọng./.

Nơi nhận:
- Như trên;
- Trung tâm Dữ liệu y tế (để thực hiện);
- Lưu: VT, CNTT.

CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN
BỘ Y TẾ

Đỗ Trường Duy

BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

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

THÔNG TIN LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số 106 */CNTT-YTĐT ngày* 18 */* 02*/2022*
của Cục 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