UBND TỈNH HÀ NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 127 /STTTT-BCVTCNTT

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 Nam, ngày 28 tháng 01 năm 2022

Kính gửi:

- Văn phòng Tỉnh ủy Hà Nam;
- Các sở, ban, ngành, cơ quan, đoàn thể của tỉnh;
- UBND các huyện, thị xã, thành phố.

Căn cứ Công văn số 144/CATTT-NCSC ngày 27/01/2022 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông về lỗ hổng bảo mật CVE-2021-4034 trong Polkit pkexec ảnh hưởng nghiêm trọng đến hệ điều hành Linux;

Nhằm tăng cường công tác bảo đảm an toàn, an ninh thông tin, đặc biệt là bảo vệ các hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị:

- Kiểm tra, rà soát và xác minh 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 *(Chi tiết tại phụ lục kèm theo)*.

- 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.

- Báo cáo kết quả việc thực hiện kiểm tra, rà soát và xử lý lỗ hổng về Sở Thông tin và Truyền thông **trước ngày 20/02/2022** để sở tổng hợp báo cáo Bộ Thông tin và Truyền thông.

Đầu mối liên hệ, hỗ trợ:

- Sở Thông tin và Truyền thông (Trung tâm Công nghệ thông tin và Truyền thông - Bộ phận thường trực Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Hà Nam). Điện thoại: **0226.3846333**. Email: **ttcntt@hanam.gov.vn**

- Trung tâm Giám sát an toàn thông tin mạng quốc gia (NCSC), Cục An toàn thông tin. Điện thoại di động: **0243.2091616**. Email: **ais@mic.gov.vn**./.

Nơi nhận:
- Như trên;
- Lưu VT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XHCN VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH HÀ NAM

Nguyễn Đức Cường

Phụ lục

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

(Kèm theo Công văn số /STTTT-BCVTCNTT ngày /01/2022 của Sở Thông tin và Truyền thông Hà Nam)

1. Thông tin lỗ hổng bảo mật

- CVSS: 7.8 (cao)

- Mô tả: Lỗ hổng này 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 lỗ hổng là cập nhật bản vá cho lỗ hổng bảo mật nói trên. Tuy nhiên trong trường hợp chưa thể cập nhật, 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

```
smod | 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