UBND TỈNH ĐỒNG NAI
SỞ Y TẾ

Số: 1390 /SYT-VP
V/v triển khai thực hiện Công văn số 106/CNTT-YTĐT và 109/CNTT-YTĐT ngày 18/02/2022 của Cục CNTT Bộ Y tế.

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

Đồng Nai, ngày 22 tháng 02 năm 2022

Kính gửi: Giám đốc, Thủ trưởng các đơn vị trực thuộc.

Thực hiện Công văn số 106/CNTT-YTĐT ngày 18/02/2022 về việc lỗ hổng bảo mật CVE-2021-4034 trong Polkit pkexec ảnh hưởng nghiêm trọng đến hệ điều hành Linux và Công văn số 109/CNTT-YTĐT ngày 18/02/2022 về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2022 của Cục Công nghệ thông tin Bộ Y tế (*đính kèm Công văn*).

Giám đốc Sở Y tế đề nghị Giám đốc, Thủ trưởng các đơn vị trực thuộc chỉ đạo các tổ chức, cá nhân phụ trách về công nghệ thông tin của đơn vị tổ chức triển khai thực hiện nội dung Công văn số 106/CNTT-YTĐT và Công văn số 109/CNTT-YTĐT ngày 18/02/2022 của Cục Công nghệ thông tin Bộ Y tế.

Đề nghị Giám đốc, Thủ trưởng các đơn vị trực thuộc triển khai thực hiện theo sự chỉ đạo./.

Nơi nhận:
- Như trên;
- Lưu: VT,VP.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ Y TẾ
TỈNH ĐỒNG NAI

Phan Huy Anh Vũ

Số 2 - Phan Đình Phùng, phường Quang Vinh, thành phố Biên Hoà, tỉnh Đồng Nai
ĐT: (02513) 942641, Fax: (02513) 847269, Email: syt@dongnai.gov.vn, Website: syt.dongnai.gov.vn

BỘ Y TẾ **CỤC CÔNG NGHỆ THÔNG TIN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
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	*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

BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

Số: 109 /CNTT-YTĐT
V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2022

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 163 /CATTT-NCSC ngày 09/02/2022 của Cục An toàn thông tin về lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2022.

Ngày 08/02/2022, Microsoft đã phát hành danh sách bản vá tháng 02 với 48 lỗ hổng bảo mật trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý các lỗ hổng bảo mật có mức ảnh hưởng cao sau:

- Lỗ hổng bảo mật **CVE-2022-22005** trong Sharepoint Server 2013-2019 cho phép đối tượng tấn công thực thi mã từ xa với tài khoản xác thực hợp lệ.

- Lỗ hổng bảo mật **CVE-2022-21989** trong Windows Kernel cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-21984** trong DNS Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-21995** trong Windows Hyper-V cho phép đối tượng tấn công đã xác thực trên máy khách Hyper-V có thể thực thi mã từ xa trên máy chủ Hyper-V.

- 02 lỗ hổng bảo mật **CVE-2022-22718, CVE-2022-21999** trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- 02 lỗ hổng bảo mật **CVE-2022-22000, CVE-2022-21981** trong Windows Common Log File System Driver cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-21996** trong Windows32k cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-22715** trong Named Pipe File System cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

Thông tin chi tiết các 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, Cục Công nghệ thông tin trân trọng đề nghị Quý đơn vị:

1. Kiểm tra, rà soát, xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công (tham khảo thông tin tại phụ lục kèm theo).

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, 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 109 */CNTT-YTĐT ngày* 18 */02/2022*
của Cục Công nghệ thông tin)

1. Thông tin lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-22005	- Điểm CVSS: 8.8 (cao) - Lỗ hổng trong Microsoft SharePoint Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2019, SharePoint Enterprise Server 2013/2016.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22005
2	CVE-2022-21989	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Microsoft Kernel, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2022/2019/2016/2012/20 - 08, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21989
3	CVE-2022-21984	- Điểm CVSS: 8.8 (cao) - Lỗ hổng trong Windows DNS Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows - 10/11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21984

4	CVE-2022-21995	- Điểm CVSS: 7.9 (cao) - Lỗ hổng trong Windows Hyper-V, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10/11, Windows Server - 2022/2019/2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21995
5	CVE-2022-22718	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Print Sooler, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2022/2016/2012/2008, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22718
6	CVE-2022-22000	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Common Log File System Driver, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows Server 2022/2019/2016/2012/20 - 08, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22000
7	CVE-2022-21999	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Print Sooler, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows Server 2022/2016/2012/2008, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21999

8	CVE-2022-21981	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Common Log File System Driver, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai - thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows Server 2019/2012/2008, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21981
9	CVE-2022-21996	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows32k, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows 11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21996
10	CVE-2022-22715	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Named Pipe File System, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows - 11/10, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22715

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng bảo mật nói trên theo hướng dẫn của hãng. Quý đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo tại mục 1 của phụ lục.

3. Tài liệu tham khảo

https://msrc.microsoft.com/update-guide/

https://www.zerodayinitiative.com/blog/2022/2/8/the-february2022-security-update-review