UBND TỈNH TUYÊN QUANG **SỞ THÔNG TIN VÀ TRUYỀN THÔNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh Phúc**
Số: 393 /STTTT-CNTT&BCVT V/v lỗ hổng bảo mậtcó mức ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 4/2022	*Tuyên Quang, ngày18 tháng 4 năm 2022*

Kính gửi:

- Văn phòng Hội đồng nhân dân tỉnh;
- Văn phòng Ủy ban nhân dân tỉnh;
- Các sở, ban, ngành;
- Uỷ ban nhân dân các huyện, thành phố;
- Trung tâm Công nghệ thông tin và Truyền thông, Sở Thông tin và Truyền thông.

Căn cứ văn bản số 508/CATTT – NCSC ngày 13/4/2022 của Cục An toàn thông tin về việc lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 4/2022;

Sở Thông tin và Truyền thông cảnh báo tới các cơ quan, đơn vị, thông tin cụ thể như sau:

I. Thông tin về lỗ hổng bảo mật trong các sản phẩm Microsoft

Ngày 12/04/2022, Microsoft đã phát hành danh sách bản vá tháng 4với 128 lỗ hổng bảo mật trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý sau:

Các lỗ hổng bảo mật có mức ảnh hưởng Nghiêm trọng:

- Lỗ hổng bảo mật CVE-2022-26809 trong RPC Runtime Library cho phép đối tượng tấn công thực thi mã từ xa với đặc quyền cao trên hệ thống bị ảnh hưởng

- 02 lỗ hổng bảo mật CVE-2022-24491,CVE-2022-24497 trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa với đặc quyền cao.

Các lỗ hổng bảo mật có mức ảnh hưởng Cao:

- Lỗ hổng bảo mật CVE-2022-26815trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2022-26904trong Windows User Profile Service cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đã có mã khai thác công khai trên Internet.

- Lỗ hổng bảo mật CVE-2022-26919 trong Windows LDAP cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2022-24521 trong Windows Common Log File System Driver 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).

II. Các giải pháp phòng tránh

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý cơ quan đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông đề nghị các sở, ban, ngành, Ủy ban nhân dân các huyện, thành phố triển khai thực hiện:

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.

3.Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Ban Giám đốc sở (báo cáo);
- Lưu: VT, CNTT&BCVT

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TUYÊN QUANG

Nguyễn Văn Hiến

Phụ lục

Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft

(Kèm theo Công văn số 393 /STTTT-CNTT&BCVT ngày 18 /4/2022 của Sở Thông tin và Truyền thông)

1.Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-26809	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong RPC Runtime Library cho phép đối tượng tấn công thực thi mã từ xa với đặc quyền cao trên hệ thống bị ảnh hưởng. - Ảnh hưởng: Windows 7/8.1/10/11,Windows Server 2008/2012/2016/2019/2022	https://msrc.microsf.com/updateguide/vulnerability/CVE-2022-26809
2	CVE-2022-24491	- Điểm CVSS: 98 (Nghiêm trọng) - Lỗ hổng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa với đặc quyền cao. - Ảnhhưởng:Windows 8.1/10/11,Windows Server2012/2016/2019.	https://msrc.microsoft.com/update-guidevulnerability/CVE-2022-24491
3	CVE-2022-24497	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10, Windows Server 2012/2016/2019/2022.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-24497
4	CVE-2022-26815	- Điểm CVSS: 7.2 (cao) -Lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26815

		- Ảnh hưởng: Windows Server2008/2012/2016/2019/ 2022	
5	CVE-2022-26904	- Điểm CVSS: 7.9 (cao) - Lỗ hổng trong Windows User Profile Service cho Phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã có mã khai thác công khai trên Internet. -Ảnh hưởng: Windows 7/8.1/10/11,Windows Server 2008/2012/2016. -	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26904
6	CVE-2022-26919	- Điểm CVSS: 8.1 (Cao) - Lỗ hổng trong Windows LDAP cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2008/2012/2016/2019/20 22.	https://msrc.microsoft.com/update-guide/vulnerability/C V E-2022-26919.
7	CVE-2022-24521	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Common Log File System Driver cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11,Windows Server 2008/2012/2016/2019/20 22.	https://msrc.microsoft.com/update-guide/enUS/vulnerability/CVE-2022-24521

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/releaseNote/2022-Apr

https://www.zerodayinitiative.com/blog/2022/4/11/the-april-2022-security-update-review