ỦY BAN NHÂN DÂN **HUYỆN CẨM XUYÊN**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 936 /UBND-VHTT Về việc cảnh báo lỗ hổng bảo mật có mức ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 04/2022	*Cẩm Xuyên, ngày18 tháng 4 năm 2022*

Kính gửi:

- Các phòng, ban, cơ quan đoàn thể cấp huyện;
- Ủy ban nhân dân các xã, thị trấn;
- Các đơn vị trường học đóng trên địa bàn.

Thực hiện Công văn số 411/STTTT-TTCNTT ngày 15/4/2022 của Sở Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật có mức ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 04/2022. Để đảm bảo an toàn thông tin mạng trong các cơ quan nhà nước trên địa bàn, UBND huyện yêu cầu các phòng, ban, cơ quan, đoàn thể cấp huyện; UBND các xã, thị trấn, các đơn vị trường học (gọi tắt là các đơn vị) thực hiện các nội dung sau:

1. Kiểm tra, rà soát và xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Nếu có, thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công theo hướng dẫn tại Văn bản số 508/CATTT-NCSC ngày 14/4/2022 của Cục an toàn thông tin *(có văn bản 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; thực hiện cài đặt các phần mềm virut có bản quyền…

Nhận được Công văn yêu cầu các đơn vị triển khai nghiêm túc thực hiện./.

Nơi nhận: - Như trên; - TTr. Huyện ủy - HĐND huyện; - Chủ tịch, các PCT UBND huyện; - Cổng TTĐT huyện; - Lưu: VT, VHTT.	**TM. ỦY BAN NHÂN DÂN** **KT. CHỦ TỊCH** **PHÓ CHỦ TỊCH** **Phạm Văn Thắng**

Phụ lục

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

(Kèm theo Công văn số 936 /CATTT-NCSC ngày / /2022 của Cục An toàn thông tin)

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. micro soft. com/update-guide/vulnerability/CVE-2022-26809
2	CVE-2022-24491	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa với đặc quyền cao. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019.	https: //msrc. micro soft. com/update-guide/vulnerability/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. micro soft. com/update-guide/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. micro soft. com/update-guide/vulnerability/CVE-2022-26815

		- Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022.	
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 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-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 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/en-US/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/2022/4Z11/the-april-2022-security-update-review