ỦY BAN NHÂN DÂN **HUYỆN TÂY SƠN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1010/UBND-VX V/v cảnh báo lỗ hổng bảo mật trong các sản phẩm Microsoft tháng 7/2022	*Tây Sơn, ngày 21 tháng 07 năm 2022*

Kính gửi:
- Các phòng, ban, ngành thuộc huyện;
- UBND các xã, thị trấn.

Theo đề nghị của Sở Thông tin và Truyền thông tại Văn bản số 746/STTTT-BCVT&CNTT ngày 18/7/2022 về việc cảnh báo lỗ hổng bảo mật trong các sản phẩm Microsoft tháng 7/2022. Để bảo đảm an toàn thông tin cho hệ thống thông tin của cơ quan, đơn vị, địa phương, góp phần bảo đảm an toàn cho các hoạt động trên môi trường mạng, Chủ tịch UBND huyện đề nghị thủ trưởng các phòng, ban, ngành, chủ tịch UBND các xã, thị trấn triển khai thực hiện các nội dung sau:

1. Chỉ đạo 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 (có Phụ lục hướng dẫn gửi kèm).

2. Tăng cường giám sát hệ thống mạng tại cơ quan, đơn vị để kịp thời phát hiện hoạt động tấn công mạng; phối hợp với Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh, phòng chuyên môn của huyện trong xử lý, ứng cứu sự cố mất an toàn thông tin khi tham gia hoạt động trên môi trường mạng tại cơ quan, đơn vị.

Trong quá trình triển khai nếu cần hỗ trợ liên hệ Phòng Bưu chính, Viễn thông và Công nghệ thông tin thuộc Sở Thông tin và Truyền thông, điện thoại: 0256.2210517.

Đề nghị các phòng, ban, ngành thuộc huyện, UBND các xã, thị trấn triển khai thực hiện./.

Nơi nhận:
- Như trên;
- CT, các PCT UBND huyện;
- CVP, PVP, C3;
- Lưu: VT.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Bùi Văn Mỹ

Phụ lục
Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft
(*Kèm theo Công văn số /UBND-VX ngày /7/2022 của Ủy ban nhân dân huyện*)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-22047	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Client Server Run-Time Subsystem cho phép đối tượng tấn công thực hiện leo thang đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11. Windows Server 2008/2012.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22047
2	CVE-2022-30216	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Windows Server Service cho phép đối tượng tấn công cài chứng chỉ giả mạo độc hại lên máy chủ mục tiêu từ đó có thể thực hiện các dạng tấn công khác bao gồm tấn công chiếm quyền điều khiển. - Ảnh hưởng: Windows 10/11, Windows Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30216
3	CVE-2022-22029	- Điểm CVSS: 8.1 (Cao) - Lỗ hổng trong trong Windows Network File System cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/20 22.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22029
4	CVE-2022-22039	- Điểm CVSS: 7.5 (Cao) - Lỗ hổng trong trong Windows Network File System cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE 2022-22039

5	CVE-2022-22038	- Điểm CVSS: 8.1 (Cao) - Lỗ hổng trong trong Remote Procedure Call Runtime cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22038
6	CVE-2022-30206	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 7/8.1/10, Windows Server 2008/2012/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30206
7	CVE-2022-22022	- Điểm CVSS: 7.1 (Cao) - Lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2016/2019/2022.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE2022-22022
8	CVE-2022-30226	- Điểm CVSS: 7.1 (Cao) - Lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công leo thang đặcquyền. - Ảnh hưởng: Windows 7/8.1/10/12, Windows Server 2008/2012/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30226
9	CVE-2022-22041	- Điểm CVSS: 6.8 (Cao) - Lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 8.1/10, Windows Server 2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE2022-22041

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. Các cơ quan, đơn vị, địa phương 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-Jul

https://www.zerodayinitiative.com/blog/2022/7/12/the-july-2022-security-update-review