ỦY BAN NHÂN DÂN **HUYỆN TÂY SƠN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 69 /UBND-VX	*Tây Sơn, ngày 19 tháng 01 năm 2022*

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2022

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 55/STTTT-BCVT&CNTT ngày 17/01/2022 về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2022. Để bảo đảm an toàn thông tin cho hệ thống thông tin của cơ quan, đơn vị, địa phương và trên không gian 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 trường hợp xảy ra sự cố mất an toàn thông tin khi hoạt động trên môi trường mạng.

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, C2; - 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 /01/2022 của Ủy ban nhân dân huyện*)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-21907	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong HTTP Protocol, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2019/2022, Windows 11/10.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21907
2	CVE-2022-21846	- Điểm CVSS: 9.0 (Cao) - Lỗ hổng trong Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Exchange Server 2019/2016/2013.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21846
3	CVE-2022-21855	- Điểm CVSS: 9.0 (Cao) - Lỗ hổng trong Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Exchange Server 2019/2016/2013.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21855
4	CVE-2022-21969	- Điểm CVSS: 9.0 (Cao) - Lỗ hổng trong Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Exchange Server 2019/2016/2013.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21969
5	CVE-2022-21840	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Microsoft Office, cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21840

		- Ảnh hưởng: Microsoft SharePoint Foundation 2013, SharePoint Server 2019, Microsoft Office 2016/2013/LTSC 2021/2019, Microsoft Excel 2016/2013, Microsoft 365	
6	CVE-2022-21875	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Active Directory Domain Services, cho phép đối tượng tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2022/2019/2016/2012/2008, Windows 11/10/RT 8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21857
7	CVE-2022-21911	- Điểm CVSS: 7.5 (Cao) - Lỗ hổng trong .NET Framework, cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. - Ảnh hưởng: Microsoft .NET Framework 3.5 AND 4.7.2, 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2,…	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21911
8	CVE-2022-21836	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Certificate, cho phép đối tượng tấn công thực hiện tấn công giả mạo - Ảnh hưởng: Windows Server 2022/2019/2016/2012/2008, Windows 10/RT 8.1/7.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21836
9	CVE-2022-21841	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Microsoft Excel, cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21841

		- Ảnh hưởng: Microsoft Office 2013/2016/2019/LTSC2021, Microsoft 365.	
10	CVE-2022-21837	- Điểm CVSS: 8.3 (cao) - Lỗ hổng trong Microsoft SharePoint Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2019, 2016	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21837
11	CVE-2022-21842	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Microsoft Word, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Word 2016.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21842

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-Jan

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