

**ỦY BAN NHÂN DÂN
HUYỆN TÂY SƠN**

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

Số: /UBND-VX

Tây Sơn, ngày tháng năm 2022

V/v cảnh báo lỗ hổng bảo mật
ảnh hưởng cao trong các sản phẩm
Microsoft tháng 5/2022

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 504/STTTT-BCVT&CNTT ngày 13/5/2022 về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft tháng 5/2022. 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 /5/2022
của Ủy ban nhân dân huyện)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-26925	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows LSA cho phép đối tượng tấn công không cần xác thực có thể thực hiện tấn công giả mạo (spoofing) kết hợp với NTLM relay attack từ đó nâng cao đặc quyền trong hệ thống mục tiêu. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2022/2019/2016/2012/2008	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-26925
2	CVE-2022-26923	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Active Directory Domain Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24491
3	CVE-2022-26937	- 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 Server 2008/2012/2016/2019/2022	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26937
4	CVE-2022-29972	- Lỗ hổng trong Magnitude Simba Amazon Redshift ODBC Driver cho phép đối tượng thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29972 https://msrc-blog.microsoft.com/2022/05/09/vulnerability-

			mitigated-in-the-third-party-data-connector-used-in-azure-synapse-pipelines-and-azure-data-factory-cve-2022-29972
5	CVE-2022-21978	- Điểm CVSS: 8.2 (Cao) - Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2013/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21978
6	CVE-2022-22017	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Remote Desktop Protocol Client cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22017
7	CVE-2022-29110	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office Web Apps Server 2013, Microsoft Excel 2013/2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29110
8	CVE-2022-29108	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2016/2019, Microsoft SharePoint Foundation 2013.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29108

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-May>

<https://www.zerodayinitiative.com/blog/2022/5/10/the-may-2022-security-update-review>