UỶ BAN NHÂN DÂN **HUYỆN VĂN LÂM**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 199/UBND-VHTT V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2024	*Văn Lâm, ngày 29 tháng 02 năm 2024*

Kính gửi:

- Các phòng, ban, ngành, đoàn thể huyện;
- UBND các xã, thị trấn.

Theo thông báo của Cục An toàn thông tin – Bộ Thông tin và Truyền thông về lỗ hổng an toàn thông tin ảnh hưởng Cao trong các sản phẩm Microsoft; với 72 lỗ hổng, trong đó đáng chú ý là các lỗ hổng bảo mật sau:

- Lỗ hổng an toàn thông tin **CVE-2024-21410** trong Microsoft Exchange Server cho phép đối tượng không cần xác thực thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

- 02 lỗ hổng an toàn thông tin **CVE-2024-21413**, **CVE-2024-21378** trong Microsoft Outlook cho phép đối tượng tấn công không cần xác thực thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-21399** trong Microsoft Edge (Chromium-based) cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-21412** trong Internet Shortcut Files cho phép đối tượng tấn công vượt qua cơ chế bảo mật. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2024-21379** trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-21384** trong Microsoft Office OneNote cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-20673** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-21351** trong Windows SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo mật. Lỗ hổng hiện đang bị khai thác trong thực tế.

Thực hiện Công văn số 236/STTTT-BCVTCNTT ngày 23/02/2024 của Sở Thông tin và Truyền thông Hưng Yên về lỗ hổng an toàn thông tin ảnh hưởng cao

và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2024. Để đảm bảo an toàn hệ thống thông tin dùng chung của huyện và của các cơ quan, đơn vị trên địa bàn; Ủy ban nhân dân huyện Văn Lâm yêu cầu Thủ trưởng các cơ quan, đơn vị, địa phương chỉ đạo các bộ phận chuyên môn triển khai thực hiện rà soát, khắc phục các lỗ hổng bảo mật trên theo các khuyến nghị sau:

1. Thực hiện 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 đính kèm)*

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 cần hỗ trợ cơ quan, đơn vị liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại 02432091616, thư điện tử: ais@mic.gov.vn./.

Nơi nhận:
- Như kính gửi;
- Lãnh đạo UBND huyện;
- Lưu VT.

TM. UỶ BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Hoàng Thế Vĩnh

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM CỦA MICROSOFT
(Kèm theo công văn Số /UBND-VHTT ngày tháng 01 năm 2024 của UBND huyện Văn Lâm)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	**CVE-2024-21410**	- Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng không cần xác thực thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Exchange Server 2016, 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21410
2	**CVE-2024-21413** **CVE-2024-21378**	- Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công không cần xác thực thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft Office LTSC, Microsoft 365 Apps for Enterprise, Microsoft Outlook.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21378
3	**CVE-2024-21399**	- Điểm: CVSS: 8.3 (Trung bình) - Mô tả: Lỗ hổng trong Microsoft Edge (Chromium-based) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Edge (Chromium-based).	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21399
4	**CVE-2024-21412**	- Điểm: CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng trong	https://msrc.microsoft.com/update-guide/vulnerability/CVE-

		Internet Shortcut Files cho phép đối tượng tấn công vượt qua cơ chế bảo mật. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2019, 2022.	2024-21412
5	**CVE-2024-21379**	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Word, Microsoft Office, Microsoft Office LTSC, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21379
6	**CVE-2024-21384**	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office OneNote cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21384
7	**CVE-2024-20673**	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC, Microsoft Office, Skype for Business.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20673
8	**CVE-2024-21351**	- Điểm: CVSS: 7.6 (Cao) - Mô tả: Lỗ hổng trong Windows SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo mật. Lỗ hổng	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21351

		hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022.	

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

https://www.zerodayinitiative.com/blog/2023/5/8/the-may-2023-security-update-review