UỶ BAN NHÂN DÂN **HUYỆN VĂN LÂM**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 507 /UBND-VHTT V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 4/2024	*Văn Lâm, ngày 04 tháng 5 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 147 lỗ hổng, trong đó đáng chú ý là các lỗ hổng bảo mật sau:

- Lỗ hổng an toàn thông tin **CVE-2024-20678** trong Remote Procedure Call Runtime (RPC) cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-29988** trong SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo vệ.

- 03 lỗ hổng an toàn thông tin **CVE-2024-21322**, **CVE-2024-21323**, **CVE-2024-29053** trong Microsoft Defender for IoT cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-20670** trong Outlook for Windows làm lộ lọt NTML hash, cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing).

- Lỗ hổng an toàn thông tin **CVE-2024-26256** trong thư viện nguồn mở libarchive cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-26257** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- 07 lỗ hổng an toàn thông tin **CVE-2024-26221**, **CVE-2024-26222**, **CVE-2024-26223**, **CVE-2024-26224**, **CVE-2024-26227**, **CVE-2024-26231**, **CVE-2024-26233** trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-26234** trong Proxy Driver cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing).

Thực hiện Công văn số 520/STTTT-BCVTCNTT ngày 23/4/2024 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 04/2024. 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 trên;
- 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 AN TOÀN THÔNG TIN TRONG SẢN PHẨM MICROSOFT
(Kèm theo Công văn số /UBND-VHTT ngày /03/2024 của UBND huyện Văn Lâm)

1. Thông tin về các lỗ hổng an toàn thông tin

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-20678	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Remote Procedure Call Runtime (RPC) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20678
2	CVE-2024-29988	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29988
3	CVE-2024-21322 CVE-2024-21323 CVE-2024-29053	- Điểm: CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Defender for IoT cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Defender for IoT.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21322 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21323 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29053
4	CVE-2024-20670	- Điểm: CVSS: 8.1 (Cao)	https://msrc.microsoft.com/up

		- Mô tả: Lỗ hổng trong Outlook for Windows làm lộ lọt NTML hash, cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). - Ảnh hưởng: Outlook for Windows.	date-guide/vulnerability/CVE-2024-20670
5	CVE-2024-26256	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong thư viện nguồn mở libarchive 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-2024-26256
6	CVE-2024-26257	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft 365 Apps for Enterprise, Microsoft Office LTSC for Mac.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26257

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng an toàn thông tin 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/2024/4/9/the-april-2024-security-updates-review