

**ỦY BAN NHÂN DÂN
THỊ XÃ MỸ HÀO**

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

Số: /UBND-VHTT
V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2023

Mỹ Hào, ngày tháng năm 2023

Kính gửi: Các cơ quan, đơn vị, địa phương trên địa bàn thị xã.

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 và nghiêm trọng trong các sản phẩm Microsoft, với 103 lỗ hổng an toàn thông tin trong các sản phẩm của Microsoft. Trong đó đáng chú ý các lỗ hổng bảo mật sau:

- Lỗ hổng an toàn thông tin CVE-2023-36778 trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa;
- Lỗ hổng an toàn thông tin CVE-2023-36563 trong Microsoft WordPad cho phép đối tượng tấn công thực hiện thu thập thông tin mã băm NTLM của người dùng. Lỗ hổng hiện đang bị khai thác trong thực tế;
- Lỗ hổng an toàn thông tin CVE-2023-41763 trong Skype for Business cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế;
- 02 lỗ hổng an toàn thông tin CVE-2023-35349, CVE-2023-36697 trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa;
- Lỗ hổng an toàn thông tin CVE-2023-36434 trong Windows IIS Server cho phép đối tượng tấn công thực hiện leo thang đặc quyền.

Thực hiện Công văn số 1389/STTTT-BCVTCNTT ngày 20/10/2023 của Sở Thông tin và Truyền thông tỉnh Hưng Yên về lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2023. UBND thị xã yêu cầu các cơ quan, đơn vị, địa phương triển khai thực hiện rà soát, khắc phục lỗ hổng bảo mật trên theo 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 hướng dẫn gửi kèm Công văn*).
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 hỗ trợ các cơ quan, đơn vị, địa phương 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.

Ủy ban nhân dân thị xã yêu cầu các cơ quan, đơn vị, địa phương nghiêm túc thực hiện./.

Nơi nhận:

- Như trên;
- Chủ tịch, các Phó Chủ tịch UBND thị xã;
- Lưu: VT, VHTT.

**TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**

Nguyễn Quốc Khánh