ỦY BAN NHÂN DÂN THỊ XÃ MỸ HÀO	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1430 /UBND-VHTT V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 9/2023	*Mỹ Hào, ngày 29 tháng 9 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 59 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-2023-36761 trong Microsoft Word cho phép đối tượng tấn công thu thập thông tin về mã băm NTLM của người dùng. Lỗ hổng này hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin CVE-2023-29332 trong dịch vụ Microsoft Azure Kubernetes Service cho phép đối tượng tấn công không cần xác thực thực hiện tấn công leo thang đặc quyền.

- Lỗ hổng an toàn thông tin CVE-2023-38148 trong Internet Connection Sharing (ICS) cho phép đối tượng tấn công không cần xác thực thực thi mã từ xa khi ICS được kích hoạt.

- Lỗ hổng an toàn thông tin CVE-2023-36802 trong Streaming Service Proxy cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. Lỗ hổng này hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin CVE-2023-38146 trong Windows Themes cho phép đối tượng tấn công thực thi mã từ xa.

- 04 lỗ hổng an toàn thông tin CVE-2023-36792, CVE-2023-36793, CVE-2023-36794, CVE-2023-36796 trong Visual Studio cho phép đối tượng tấn công thực thi mã từ xa.

- 03 lỗ hổng an toàn thông tin CVE-2023-36744, CVE-2023-36745, CVE-2023-36756 trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.

Thực hiện Công văn số 1246/STTTT-BCVTCNTT ngày 25/9/2023 của Sở Thông tin và Truyền thông tỉnh Hưng Yên về lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 9/2023. 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.

Uỷ 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

Ký bởi: Ủy ban Nhân dân Thị xã Mỹ Hào
Thời gian ký: 29/09/2023 08:13:27

Nguyễn Quốc Khánh