UBND TỈNH HƯNG YÊN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 1111/STTTT-BCVTCNTT
V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 8/2023

Hưng Yên, ngày22 tháng 8 năm 2023

Kính gửi:
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các sở, ban, ngành tỉnh;
- UBND các huyện, thị xã, thành phố.

Theo thông báo của Cục An toàn thông tin – Bộ Thông tin và Truyền thông về lỗ hổng bảo mật ảnh hưởng Cao trong các sản phẩm Microsoft, với 74 lỗ hổng bảo mật trong các sản phẩm của Microsoft. Trong đó đáng chú ý các lỗ hổng bảo mật sau:

- Lỗ hổng an toàn thông tin **CVE-2023-38181** trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện tấn công Spoofing. Đối tượng tấn công có thể khai thác lỗ hổng này để vượt qua bản vá cho một lỗ hổng đã bị khai thác trong thực tế, CVE-2022-41082

- Lỗ hổng an toàn thông tin **CVE-2023-21709** trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- 04 lỗ hổng an toàn thông tin **CVE-2023-35368, CVE-2023-38185, CVE-2023-35388, CVE-2023-38182** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.

Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin, đã phát hành các văn bản cảnh báo diện rộng về những lỗ hổng ảnh hưởng đến Microsoft Exchange Server. Điều này cho thấy Microsoft Exchange Server vẫn luôn là mục tiêu hàng đầu được các đối tượng tấn công có chủ đích nhắm đến. Vì vậy, để đảm bảo an toàn thông tin cho hệ thống của các cơ quan, tổ chức, Cục An toàn thông tin trân trọng đề nghị các đơn vị rà soát lỗ hổng liên quan đến Microsoft Exchange Server để phát hiện và có phương án xử lý kịp thời, đồng thời tăng cường giám sát nhằm giảm thiểu nguy cơ bị tấn công thông qua các lỗ hổng này.

- 03 lỗ hổng an toàn thông tin **CVE-2023-35385, CVE-2023-36910, CVE-2023-36911** trong Microsoft Message Queuing cho phép đối tượng tấn công

thực thi mã từ xa.

- 02 lỗ hổng an toàn thông tin **CVE-2023-29328, CVE-2023-29330** trong Microsoft Teams cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-36895** trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-36896** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-35371** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

Để đảm bảo an toàn thông tin cho hệ thống thông tin dùng chung của tỉnh và của các cơ quan, đơn vị trên địa bàn tỉnh, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông đề nghị Quý cơ quan chỉ đạo bộ phận chuyên môn 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 kèm theo Công văn số 1500/CATTT-NCSC gửi 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 Quý cơ quan 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.

Sở Thông tin và Truyền thông đề nghị Quý cơ quan quan tâm chỉ đạo và phối hợp tổ chức thực hiện./.

Nơi nhận:
- Như kính gửi;
- UBND tỉnh (thay báo cáo);
- Công an tỉnh (để biết);
- Giám đốc, Phó Giám đốc Sở (đc Quang);
- Lưu: VT, BCVTCNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ XH CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH HƯNG YÊN

Đỗ Đình Quang