UBND TỈNH QUẢNG BÌNH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 1931 /STTTT-TTCNTT
V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2023

Quảng Bình, ngày 20 tháng 10 năm 2023

Kính gửi:

- Văn phòng Tỉnh ủy, Văn phòng Đoàn ĐBQH&HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các sở, ban, ngành, tổ chức đoàn thể cấp tỉnh;
- UBND các huyện, thị xã, thành phố.

Sở Thông tin và Truyền thông nhận được Công văn số 1850/CATTT-NCSC ngày 19/10/2023 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2023.

Theo đó, ngày 10/10/2023 Microsoft đã phát hành danh sách bản vá tháng 10 với 103 lỗ hổng an toàn thông tin trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý vào các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng 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.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý cơ quan, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông đề nghị Quý cơ quan quan tâm chỉ đạo, thực hiện:

1. Kiểm tra, rà soát, xác định các máy tính 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 *(chi tiết tại phụ lục của Công văn số 1850/CATTT-NCSC kèm theo văn bản này)*.

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.

Trong trường hợp cần hỗ trợ, Quý cơ quan liên hệ Trung tâm Công nghệ thông tin và Truyền thông thuộc Sở Thông tin và Truyền thông *(Đơn vị thường trực Đội Ứng cứu sự cố an toàn thông tin mạng của tỉnh)*; điện thoại: 0232.3846345; email: ungcuusuco@quangbinh.gov.vn.

Rất mong được sự quan tâm, phối hợp của Quý cơ quan./.

Nơi nhận:
- Như trên;
- Lãnh đạo Sở;
- Phòng CĐS;
- Lưu: VT, TTCNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH QUẢNG BÌNH

Nguyễn Xuân Ngọc