

UBND TỈNH LẠNG SƠN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: /STTTT-TTCNS
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao
và nghiêm trọng trong các sản phẩm
Microsoft công bố tháng 12/2023.

Lạng Sơn, ngày 20 tháng 12 năm 2023

Kính gửi:

- Văn phòng UBND tỉnh;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Các Sở, ban, ngành;
- Công an tỉnh (Phòng PA03, PA05);
- UBND các huyện, thành phố;
- Các cơ quan đảng, đoàn thể;
- Các tổ chức chính trị - xã hội.
- Các Doanh nghiệp Viễn thông, Ngân hàng
và các tổ chức tài chính trên địa bàn tỉnh.

Sở Thông tin và Truyền thông nhận được Công văn số 2260/CATTT-NCSC ngày 18/12/2023 của Cục An toàn thông tin về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2023, theo đó: Ngày 12/12/2023, Microsoft đã phát hành danh sách bản vá tháng 12 với 33 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-2023-36019 trong Microsoft Power Platform Connector cho phép đối tượng tấn công thực hiện tấn công giả mạo, dẫn tới thực thi mã từ xa ở phía người dùng.
- 02 lỗ hổng an toàn thông tin CVE-2023-35630, CVE-2023-35641 trong Internet Connection Sharing (ICS) cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin CVE-2023-35628 trong Windows MSHTML Platform cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin CVE-2023-35636 trong Microsoft Outlook làm lộ loạt NTML hash, 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 các cơ quan, đơn vị và góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị thực hiện:

1. 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 (*hướng dẫn chi tiết tham khảo 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.

Trong quá trình thực hiện nếu có khó khăn, vướng mắc đề nghị liên hệ với Trung tâm Công nghệ số thuộc Sở Thông tin và Truyền thông, số điện thoại 02053.818.657 để được hỗ trợ./.

Nơi nhận:

- Như trên;
- Lãnh đạo Sở;
- Phòng CDS;
- Lưu: VT, TTCNS.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Nguyễn Trọng Hùng