UBND TỈNH LẠNG SƠN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 2252 /STTTT-TTCNS
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 9/2023.

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

Lạng Sơn, ngày 25 tháng 9 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 1664/CATTT-NCSC ngày 21/9/2023 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 9/2023, theo đó: Ngày 12/9/2023, Microsoft đã phát hành danh sách bản vá tháng 9 với 59 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-2023-36761** 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.

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 CĐS;
- Lưu: VT, TTCNS.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH LẠNG SƠN

Nguyễn Trọng Hùng