

Số: /PVHTT-ATTT  
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng  
cao và nghiêm trọng trong các sản phẩm  
Microsoft công bố tháng 11/2023

Văn Quan, ngày tháng 11 năm 2023

Kính gửi:

- Các cơ quan, ban, ngành, đoàn thể huyện;
- Các tổ chức chính trị - xã hội huyện;
- UBND các xã, thị trấn.

Ngày 22/11/2023, Cục an toàn thông tin đã có Công văn số 2074/CATTT-NCSC về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 11/2023, theo đó: Ngày 14/11/2023, Microsoft đã phát hành danh sách bản vá tháng 11 với 63 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-2023-36397 trong Windows Pragmatic General Multicast cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa.

- Lỗ hổng an toàn thông tin CVE-2023-36400 trong Windows HMAC Key Derivation cho phép đối tượng tấn công thực hiện leo thang đặc quyền.

- Lỗ hổng an toàn thông tin CVE-2023-36025 cho phép đối tượng tấn công vượt qua tính năng bảo mật SmartScreen của Windows. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin CVE-2023-36038 trong ASP.NET Core cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ (DoS). Thông tin chi tiết về lỗ hổng đã được công bố trong thực tế.

- Lỗ hổng an toàn thông tin CVE-2023-36439 trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin CVE-2023-36033 trong Windows Desktop Manager cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin CVE-2023-36036 trong Windows Cloud Files Mini Filter Driver cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin CVE-2023-36041 trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin CVE-2023-36413 cho phép đối tượng tấn công vượt qua tính năng bảo mật của Microsoft Office. Thông tin chi tiết về lỗ hổng đã được công bố trong thực tế.

- Lỗ hổng an toàn thông tin CVE-2023-38177 trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

Thực hiện Công văn số 2867/STTTT-TTCNS ngày 23/11/2023 của Sở Thông tin và Truyền thông tỉnh Lạng Sơn, về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 11/2023; 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, Phòng Văn hóa và Thông tin huyện Văn Quan đề nghị các cơ quan, đơn vị thực hiện một số nội dung sau:

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 vướng mắc đề nghị các cơ quan, đơn vị liên hệ với Phòng Văn hóa và Thông tin huyện Văn Quan, ông Chu Quốc Tài, số điện thoại: 0912404109 để phối hợp giải quyết./.

**Nơi nhận:**

- Như trên;
- UBND huyện (b/c);
- Lãnh đạo phòng;
- Lưu: VT.

**KT. TRƯỞNG PHÒNG  
PHÓ TRƯỞNG PHÒNG**

**Hà Thị Thanh Thúy**