UBND TỈNH LAI CHÂU
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số2005 /STTTT-BCVTCNTT

Lai Châu, ngày 24 tháng 10 năm 2023

V/v Lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2023.

Kính gửi:
- Các Sở, Ban, Ngành tỉnh;
- UBND các huyện, thành phố.

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.

(Thông tin chi tiết các lỗ hổng bảo mật có tại phụ lục kèm theo).

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông khuyến nghị Quý 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 *(tham khảo thông tin tại phụ lục kèm theo)*.

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 có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ais@mic.gov.vn.

Trên đây là cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2023, kính đề nghị Quý cơ quan quan tâm thực hiện./.

Nơi nhận:
- Như trên;
- Lưu: VT, BCVTCNTT.

GIÁM ĐỐC

Ký bởi: Sở Thông tin và Truyền thông
Thời gian ký: 24/10/2023 14:12:58

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH LAI CHÂU

Nguyễn Minh Hiệu

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM CỦA MICROSOFT
(Kèm theo Công văn số /STTTT-BCVTCNTT ngày / /2023 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-36778	- Điểm: CVSS: 8.0 (Cao) - Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Exchange Server 2016, 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36778
2	CVE-2023-36563	- Điểm: CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng 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. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36563
3	CVE-2023-41763	- Điểm: CVSS: 5.3 (Cao) - Mô tả: Lỗ hổng 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. - Ảnh hưởng: Skype for Business 2015, 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-41763

STT	CVE	Mô tả	Link tham khảo
4	CVE-2023-35349 CVE-2023-36697	- Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35349 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36697
5	CVE-2023-36434	- Điểm: CVSS: 9.8 (Cao) - Mô tả: Lỗ hổng trong Windows IIS Server cho phép đối tượng tấn công thực hiện leo thang đặc quyền. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36434

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng an toàn thông tin nói trên theo hướng dẫn của hãng. Quý đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo tại mục 1 của Phụ lục.

3. Tài liệu tham khảo

https://msrc.microsoft.com/update-guide/

https://www.zerodayinitiative.com/blog/2023/10/10/the-october-2023-security-update-review