UBND TỈNH TUYÊN QUANG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: /STTTT-CNTT&BCVT
V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 08/2023

Tuyên Quang, ngày tháng 8 năm 2023

Kính gửi:

- Văn phòng Đoàn Đại biểu Quốc hội và Hội đồng nhân dân;
- Văn phòng Ủy ban nhân dân tỉnh;
- Các sở, ban, ngành;
- Uỷ ban nhân dân các huyện, thành phố.

Căn cứ văn bản số 1500/CATTT–NCSC ngày 21/8/2023 của Cục An toàn thông tin về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoftcông bố tháng 8/2023, Sở Thông tin và Truyền thông cung cấp thông tin và đưa ra các giải pháp phòng, tránh khai thác lỗ hổng bảo mật cao và nghiêm trọng trong các sản phẩm Microsoft như sau:

I. Thông tin về lỗ hổng bảo mật trong các sản phẩm Microsoft

Ngày 08/8/2023, Microsoft đã phát hành danh sách bản vá tháng 8 với 74 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-2023-38181** trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện tấn công Spoofing. Đối tượng tấn công có thể khai thác lỗ hổng này để vượt qua bản vá cho một lỗ hổng đã bị khai thác trong thực tế, CVE-2022-41082.

- Lỗ hổng an toàn thông tin **CVE-2023-21709** trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- 04 lỗ hổng an toàn thông tin **CVE-2023-35368, CVE-2023-38185, CVE-2023-35388, CVE-2023-38182** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.

Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin, đã phát hành các văn bản cảnh báo diện rộng về những lỗ hổng ảnh hưởng đến Microsoft Exchange Server. Điều này cho thấy Microsoft Exchange Server vẫn luôn là mục tiêu hàng đầu được các đối tượng tấn công có chủ đích nhắm đến. Vì vậy, để đảm bảo an toàn thông tin cho hệ thống của các cơ quan, tổ chức, Cục An toàn thông tin trân trọng đề nghị các đơn vị rà soát lỗ hổng liên quan đến Microsoft Exchange Server để phát hiện và có phương án xử lý kịp thời, đồng thời tăng cường giám sát nhằm giảm thiểu nguy cơ bị tấn công thông qua các lỗ hổng này.

- 03 lỗ hổng an toàn thông tin **CVE-2023-35385, CVE-2023-36910, CVE-2023-36911** trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa.

- 02 lỗ hổng an toàn thông tin **CVE-2023-29328, CVE-2023-29330** trong Microsoft Teams cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-36895** trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-36896** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-35371** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

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

II. Các giải pháp phòng tránh

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 đơn vị thực hiện:

1. Kiểm tra, rà soát, xác định 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 (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: ncsc@ais.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Ban Giám đốc sở (báo cáo);
- Các đơn vị thuộc Sở;
- Lưu: VT, CNTT&BCVT

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Nguyễn Văn Hiến

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG AN TOÀN THÔNG TIN TRONG SẢN PHẨM MICROSOFT
(Kèm theo Công văn số /STTTT-CNTT&BCVT ngày / 8 /2023 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng an toàn thông tin

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-38181	- Điểm: CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện tấn công Spoofing. - Ảnh hưởng: Exchange Server 2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38181
2	CVE-2023-21709	- Điểm: CVSS: 9.8 (được Microsoft đánh giá là Cao) - Mô tả: lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Exchange Server 2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21709
3	CVE-2023-35368 CVE-2023-38185 CVE-2023-35388 CVE-2023-38182	- Điểm: CVSS: 8.0/8.8 (Cao) - Mô tả: lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Exchange Server 2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35368 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38185 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35388 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38182

STT	CVE	Mô tả	Link tham khảo
4	CVE-2023-35385 CVE-2023-36910 CVE-2023-36911	- 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 10/11, Windows Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35385 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36910 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911
5	CVE-2023-29328 CVE-2023-29330	- Điểm: CVSS: 8.8 (được Microsoft đánh giá là Nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Teams cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Teams dành cho iOS, Mac, Android, Desktop	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29328 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29330
6	CVE-2023-36895	- Điểm: CVSS: 7.8 (được Microsoft đánh giá là Nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36895
7	CVE-2023-36896	- Điểm: CVSS: 7.8 (Cao) - Mô tả: lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Excel, Office, Office LTSC, 365 Apps.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36896

STT	CVE	Mô tả	Link tham khảo
8	CVE-2023-35371	- Điểm: CVSS: 7.8 (Cao) - Mô tả: lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Office LTSC, 365 Apps.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35371

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/2023/8/8/the-august-2023-security-update-review