UBND TỈNH BÌNH THUẬN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1458 /STTTT-TTCNTT&TT
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 8/2023

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

Bình Thuận, ngày 23 tháng 8 năm 2023

Kính gửi:
- Các Sở, ban, ngành;
- UBND các huyện, thị xã, thành phố.

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.

- 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)

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị, địa phương. Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị, địa phương quan tâm triển khai thực hiện như sau:

1. Những lỗ hổng ảnh hưởng đến 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, 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.

2. Kiểm tra, rà soát, xác định máy vi tính của người dùng tại đơn vị mình có cài đặt, sử dụng các các sản phẩm Microsoft nêu trên và thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công (tham khảo thông tin tại Phụ lục kèm theo)

3. 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 triển khai thực hiện, nếu có khó khăn vướng mắc, các cơ quan, đơn vị liên hệ số điện thoại: 0252.3750293 gặp Đ/c Lê Đăng Khoa hoặc Đ/c Lê Phúc Lợi.

Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị quan tâm phối hợp thực hiện.

Trân trọng./.

Nơi nhận:
- Như trên;
- Lãnh đạo Sở;
- TT CNTT;
- Lưu: VT, TTCNTT&TT, Khoa (01b).

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH BÌNH THUẬN

Huỳnh Thanh Quang

Phụ lục

THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM MICROSOFT

(Kèm theo Công văn số /STTTT-TTCNTT&TT ngày /8/2023 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-38181	- 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
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	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29328 https://msrc.microsoft.com/upd

STT	CVE	Mô tả	Link tham khảo
		Microsoft Teams cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Teams dành cho iOS, Mac, Android, Desktop	ate-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
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 bảo mật 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