UBND TỈNH KHÁNH HÒA
TRƯỜNG CAO ĐẲNG Y TẾ

Số:474/CĐYT-TCHC
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

Khánh Hòa, ngày 05 tháng 09 năm 2023

Kính gửi: Phòng, Khoa, Bộ môn

Trường Cao đẳng Y tế Khánh Hòa nhận được công văn số 2715/STTTT-CNTTBCVT ngày 28/8/2023 của Sở Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 8/2023.

Theo thông tin tại văn bản nêu trên, 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 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.

Việc khai thác thành công lỗ hổng nêu trên có thể cho phép đối tượng thực thi mã từ xa, tấn công nâng cao đặc quyền trong hệ thống mục tiêu, từ đó có thể chiếm quyền điều khiển toàn bộ hệ thống.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Nhà trường, Ban Giám hiệu thông báo đến Phòng, Khoa, Bộ môn một số nội dung sau:

1. Kiểm tra, rà soát và xác định thiết bị 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 theo hướng dẫn của Microsoft 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; 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. Phòng, Khoa, Bộ môn thông báo nội dung văn bản này đến cán bộ, viên chức, người lao động thuộc quyền quản lý có sử dụng máy tính cá nhân phục vụ cho công việc nhà trường biết để tiến hành khắc phục. Nếu cá nhân không tự tiến hành khắc phục được thì liên hệ phòng Tổ chức – Hành chính để được hỗ trợ.

Trân trọng./.

Nơi nhận:
- Như trên (VBĐT);
- Lưu: VT.

KT.HIỆU TRƯỞNG
PHÓ HIỆU TRƯỞNG

Trần Ngọc Thành

Phụ lục

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

(Kèm theo Công văn số 474/CĐYT-TCHC ngày 05 /09 /2023 của trường Cao đẳng Y tế Khánh Hòa)

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

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 mãtừ 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

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng bảo mậtnói trên theo hướng dẫn của hãng. Các Phòng, Khoa, Bộ môn 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/2023/3/14/the-march-2023-security-update-review