UBND TỈNH KHÁNH HÒA
TRƯỜNG CAO ĐẲNG Y TẾ

Số:275/CĐYT-CNTT
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 5/2023

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

Khánh Hòa, ngày 01 tháng 06 năm 2023

Kính gửi: Phòng, Khoa, Bộ môn

Trường Cao đẳng Y tế Khánh Hòa nhận được công văn số 1571/STTTT-CNTTBCVT ngày 26/5/2023 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 5/2023.

Theo thông tin tại văn bản nêu trên, ngày 09/5/2023, Microsoft đã phát hành danh sách bản vá tháng 5 với 38 lỗ hổng bảo mật trong các sản phẩm của mình, trong đó, đáng chú ý là các lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng sau:

- Lỗ hổng bảo mật CVE-2023-24955 trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

Trong tháng 01 vừa qua, đã có hai lỗ hổng bảo mật được công bố với mã là CVE-2023-21744, CVE-2023-21742 liên quan đến Microsoft SharePoint Server, những lỗ hổng này cho phép đối tượng tấn công thực thi mã từ xa, đã được Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) cảnh báo trong văn bản số 50/CATTT-NCSC về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2023 phát hành ngày 11/01/2023. Qua đó cho thấy, Microsoft SharePoint Server đã và đang là mục tiêu nhắm đến của nhiều đối tượng tấn công mạng nhằm thực hiện các hành động trái phép. Chính vì vậy, các Phòng, Khoa, Bộ môn cần đặc biệt quan tâm và có phương án khắc phục, xử lý kịp thời nếu bị ảnh hưởng.

- 02 lỗ hổng bảo mật CVE-2023-29336, CVE-2023-24902 trong Win32k cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật CVE-2023-29325 trong Windows OLE cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đã được công bố rộng rãi trên Internet.

- Lỗ hổng bảo mật CVE-2023-24941 trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2023-24932 trong Secure Boot cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đã được công bố rộng

rãi trên Internet.

- Lỗ hổng bảo mật CVE-2023-29344 trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2023-24953 trong Microsoft Excel 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 Công nghệ thông tin để được hỗ trợ.

4. Nếu Phòng, Khoa, Bộ môn, cán bộ, viên chức, người lao động sử dụng máy tính cá nhân không liên hệ phòng Công nghệ thông tin, để xảy ra sự cố ảnh hưởng hệ thống thông tin của nhà trường thì sẽ chịu hoàn toàn trách nhiệm trước Ban giám hiệu Nhà trường.

Trân trọng./.

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

KT.HIỆU TRƯỞNG
PHÓ HIỆU TRƯỞNG

ỦY BAN NHÂN DÂN TỈNH KHÁNH HÒA
TRƯỜNG CAO ĐẲNG Y TẾ KHÁNH HÒA

Trần Ngọc Thành

Phụ lục

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

(Kèm theo Công văn số 275/CĐYT-CNTT ngày 01 /06/2023 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-2023-24955	- Điểm: CVSS: 7.2 (cao) - Mô tả: lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24955
2	CVE-2023-29336 CVE-2023-24902	- Điểm: CVSS: 7.8 (cao) - Mô tả: lỗ hổng trong Win32k cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows Server, Windows 10,11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29336 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24902
3	CVE-2023-29325	- Điểm: CVSS: 8.1 (cao) - Mô tả: lỗ hổng trong Windows OLE cho phép đối tượng tấn công thực thimã từ xa. Lỗ hổng này đã được công bố rộng rãi trên Internet. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29325
4	CVE-2023-24941	- Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hổng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24941
5	CVE-2023-24932	- Điểm: CVSS: 6.7 (trung bình) - Mô tả: lỗ hổng trong Secure Boot cho phép đối	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932

		tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đã được công bố rộng rãi trên Internet. - Ảnh hưởng: Windows Server, Windows 10/11.	
6	CVE-2023-29344	- 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, Microsoft 365.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29344
7	CVE-2023-24953	- 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 Office, Microsoft 365, Microsoft Excel.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24953

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