UBND TỈNH KHÁNH HÒA
TRƯỜNG CAO ĐẲNG Y TẾ

Số: 36 /CĐYT-CNTT
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2023

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

Khánh Hòa, ngày 03 tháng 02 năm 2023

Kính gửi: Phòng, Khoa, Bộ môn

Trường Cao đẳng Y tế Khánh Hòa nhận được công văn số 102/STTTT-CNTTBCVT ngày 13/01/2023 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 01/2023.

Theo thông tin tại văn bản nêu trên, ngày 11/01/2023, Microsoft đã phát hành danh sách bản vá tháng 01 với 98 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-2023-21674 trong Windows Advanced Local Procedure Call (ALPC) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.

- 03 lỗ hổng bảo mật CVE-2023-21743, CVE-2023-21744, CVE-2023-21742 trong Microsoft SharePoint Server, trong đó CVE-2023-21743 cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật; 02 lỗ hổng CVE-2023-21744, CVE-2023-21742 cho phép đối tượng tấn công thực thi mã từ xa.

- 04 lỗ hổng bảo mật CVE-2023-21763, CVE-2023-21764, CVE-2023-21762, CVE-2023-21745 trong Microsoft Exchange Server, trong đó 02 lỗ hổng CVE-2023- 21763, CVE-2023-21764 cho phép đối tượng tấn công thực hiện nâng cao đặc quyền; 02 lỗ hổng CVE-2023-21762, CVE-2023-21745 cho phép đối tượng tấn công thực hiện tấn công giả mạo.

- Lỗ hổng bảo mật CVE-2023-21549 trong Windows Workstation Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã được công bố rộng rãi trên Internet.

- 02 lỗ hổng bảo mật CVE-2023-21561, CVE-2023-21551 trong Microsoft Cryptographic Services cho phép đối tượng tấn công nâng cao đặc quyền.

- 02 lỗ hổng bảo mật CVE-2023-21734, CVE-2023-21735 trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa..

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 36 /CĐYT-CNTT ngày 03 /02 /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-2023-21674	- Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong Windows Advanced Local Procedure Call (ALPC) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21674
2	CVE-2023-21743, CVE-2023-21744, CVE-2023-21742	- Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass), thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21743 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21744 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21742
3	CVE-2023-21763, CVE-2023-21764, CVE-2023-21762, CVE-2023-21745	- Điểm: CVSS: 8.0/7.8 (cao) - Mô tả: lỗ hổng trong trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền, tấn công giả mạo (Spoofing). - Ảnh hưởng: Microsoft Exchange Server 2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21763 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21764 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21762

			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21745
4	CVE-2023-21549	- Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong Windows Workstation Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã được công bố rộng rãi trên Internet. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2012/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21549
5	CVE-2023-21561, CVE-2023-21551	- Điểm: CVSS: 8.8/7.8 (cao) - Mô tả: lỗ hổng trong Microsoft Cryptographic Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/ 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21561 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21551
6	CVE-2023-21734, CVE-2023-21735	- 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 LTSC for Mac 2021, Microsoft 365, Microsoft Office 2019 for Mac.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21734 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21735

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. 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/releaseNote/2022-Oct
https://www.zerodayinitiative.com/blog/2022/10/11/the-october-2022-security-update-review