UBND TỈNH KHÁNH HÒA
TRƯỜNG CAO ĐẲNG Y TẾ

Số: 567/CĐYT-TCHC
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 9/2023

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

Khánh Hòa, ngày 09 *tháng* 10 *năm 2023*

Kính gửi: Phòng, Khoa.

Trường Cao đẳng Y tế Khánh Hòa nhận được công văn số 3163/STTTT-CNTTBCVT ngày 29/9/2023 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 10/2023.

Theo thông tin tại văn bản nêu trên, ngày 21/9/2023, Microsoft đã phát hành danh sách bản vá tháng 9 với 59 lỗ hổng an toàn thông tin trong các sản phẩm của mình, trong đó, đáng chú ý là các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng sau:

- Lỗ hổng an toàn thông tin **CVE-2023-36761** trong Microsoft Word cho phép đối tượng tấn công thu thập thông tin về mã băm NTLM của người dùng. Lỗ hổng này hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-29332** trong dịch vụ Microsoft Azure Kubernetes Service cho phép đối tượng tấn công không cần xác thực thực hiện tấn công leo thang đặc quyền.

- Lỗ hổng an toàn thông tin **CVE-2023-38148** trong Internet Connection Sharing (ICS) cho phép đối tượng tấn công không cần xác thực thực thi mã từ xa khi ICS được kích hoạt.

- Lỗ hổng an toàn thông tin **CVE-2023-36802** trong Streaming Service Proxy cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. Lỗ hổng này hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-38146** trong Windows Themes cho phép đối tượng tấn công thực thi mã từ xa.

- 04 lỗ hổng an toàn thông tin **CVE-2023-36792, CVE-2023-36793, CVE-2023-36794, CVE-2023-36796** trong Visual Studio cho phép đối tượng tấn công thựcthi mã từ xa.

- 03 lỗ hổng an toàn thông tin **CVE-2023-36744, CVE-2023-36745, CVE-2023-36756** trong Microsoft Exchange Server cho phép đối tượng tấn công thựcthi 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 cơuan 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./.

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

KT.HIỆU TRƯỞNG
PHÓ HIỆU TRƯỞNG

CỤC CẢNH SÁT QUẢN LÝ HÀNH CHÍNH VỀ TRẬT TỰ XÃ HỘI
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 567/CĐYT-TCHC ngày 09 /10 /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-2023-36761	- Điểm: CVSS: 6.2 (Cao) - Mô tả: Lỗ hổng trong Microsoft Word cho phép đối tượng tấn công thu thập thông tin về mã băm NTLM của người dùng. Lỗ hổng này hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Word, Microsoft 365.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36761
2	CVE-2023-29332	- Điểm: CVSS: 7.5 (Nghiêm trọng) - Mô tả: Lỗ hổng trong dịch vụ Microsoft Azure Kubernetes Service cho phép đối tượng tấn công không cần xác thực thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Microsoft Azure Kubernetes Service.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29332
3	CVE-2023-38148	- Điểm: CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Internet Connection Sharing (ICS) cho phép đối tượng tấn công không cần xác thực thực thi mã từ xa khi ICS được kích hoạt. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38148
4	CVE-2023-36802	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Streaming Service Proxy cho	https://msrc.microsoft.com/update-

		phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng này hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 11.	guide/vulnerability/CVE-2023-36802
5	CVE-2023-38146	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Windows Themes cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38146
6	CVE-2023-36792 CVE-2023-36793 CVE-2023-36794 CVE-2023-36796	- Điểm: CVSS: 7.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Visual Studio cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft .NET Framework.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36792 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36793 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36794 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36796
7	CVE-2023-36744 CVE-2023-36745 CVE-2023-36756	- Điểm: CVSS: 8.0 (Cao) - Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Exchange Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36744 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36745 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36756

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