

Số: /CĐYT-CNTT
V/v cảnh báo lỗ hổng bảo mật ảnh
hưởng cao và nghiêm trọng trong các
sản phẩm Microsoft công bố tháng
4/2023

Khánh Hòa, ngày tháng năm 2023

Kính gửi: Phòng, Khoa, Bộ môn

Trường Cao đẳng Y tế Khánh Hòa nhận được công văn số 1185/STTTT-CNTTBCVT ngày 24/4/2023 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 4/2023.

Theo thông tin tại văn bản nêu trên, ngày 11/4/2023, Microsoft đã phát hành danh sách bản vá tháng 4 với 97 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-2023-28252 trong Windows Common Log File System Driver 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-2023-21554 trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa.

- 03 lỗ hổng bảo mật CVE-2023-23384, CVE-2023-23375, CVE-2023-28304 trong Microsoft SQL Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2013-3900 xác thực chữ ký WinVerifyTrust cho phép đối tượng tấn công có thể thêm nội dung vào phần chữ ký mã xác thực trong tệp thực thi đã ký mà không làm mất hiệu lực chữ ký. Gần đây, lỗ hổng này đã được sử dụng trong các cuộc tấn công chuỗi cung ứng vào phần mềm của hãng 3CX. Microsoft đã đưa ra bản vá về việc kiểm tra tính xác thực của chữ ký dưới dạng tùy chọn bật hoặc tắt, nếu không được cấu hình sẽ mặc định là tắt. Trong bản cập nhật này Microsoft đã bổ sung thêm các phiên bản hệ điều hành bị ảnh hưởng. Để nâng cao bảo mật an toàn thông tin cho các thiết bị sử dụng hệ điều hành Windows người dùng có thể xem xét việc bật tùy chọn kiểm tra này.

- 02 lỗ hổng bảo mật CVE-2023-28287, CVE-2023-28295 trong Microsoft

Publisher cho phép đối tượng tấn công thực thi mã từ xa.

- 02 lỗ hổng bảo mật CVE-2023-28309, CVE-2023-28314 trong Microsoft Dynamics 365 cho phép đối tượng tấn công thực hiện tấn công XSS.

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**

Trần Ngọc Thành

Phụ lục

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

(Kèm theo Công văn số /CDYT-CNTT ngày / /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-2023-28252	<ul style="list-style-type: none">- Điểm: CVSS: 7.8 (cao)- Mô tả: lỗ hổng trong Windows Common Log File System Driver 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-2023-28252
2	CVE-2023-21554	<ul style="list-style-type: none">- 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 Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21554
3	CVE-2023-23384 CVE-2023-23375 CVE-2023-28304	<ul style="list-style-type: none">- Điểm: CVSS: 7.8/7.3 (cao)- Mô tả: lỗ hổng trong Microsoft SQL Server cho phép đối tượng tấn công thực thi mã từ xa.- Ảnh hưởng: Microsoft SQL Server, Microsoft ODBC Driver 18.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23384 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23375 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28304
4	CVE-2013-3900	<ul style="list-style-type: none">- Điểm: CVSS: 7.4 (cao)- Mô tả: lỗ hổng xác thực chữ ký WinVerifyTrust cho phép đối tượng tấn công có thể thêm nội dung	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900

		vào phần chữ ký mã xác thực trong tệp thực thi đã ký mà không làm mất hiệu lực chữ ký. - Ảnh hưởng: Windows Server, Windows 10/11.	
5	CVE-2023-28287 CVE-2023-28295	- Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong Microsoft Publisher cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft Publisher.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28287 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28295
6	CVE-2023-28309 CVE-2023-28314	- Điểm: CVSS: 7.6/6.1 (cao) - Mô tả: lỗ hổng trong Microsoft Dynamics 365 cho phép đối tượng tấn công thực hiện tấn công XSS. - Ảnh hưởng: Microsoft Dynamics 365.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28309 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28314

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. 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>