UBND TỈNH KIÊN GIANG
SỞ Y TẾ

Số: 1288 /SYT-VP

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 04/2023

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

Kiên Giang, ngày 27 tháng 4 năm 2023

Kính gửi:
- Các phòng chức năng Sở Y tế;
- Các cơ quan, đơn vị thuộc và trực thuộc Sở Y tế. (tuyến huyện/tuyến tỉnh).

Thực hiện Công văn số 349/CNTT-YTĐT ngày 20/4/2023 của Cục Công nghệ thông tin, Bộ Y tế và Công văn số 719/STTTT-CĐS ngày 19/4/2023 của Sở Thông tin và Truyền thông tỉnh Kiên Giang về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 04/2023,

Để duy trì hiệu quả đảm bảo an toàn khi sử dụng máy tính tại các cơ quan, đơn vị trực thuộc, Sở Y tế đề nghị lãnh đạo các cơ quan, đơn vị thuộc và trực thuộc quan tâm triển khai thực hiện một số nội dung, cụ thể:

1. Cơ quan, đơn vị tiến hành rà soát, kiểm tra máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng bởi các lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 04/2023 *(đính kèm phụ lục hướng dẫn)*. Theo đó, Microsoft vừa phát hành danh sách bản vá lỗi tháng 04/2023 với 97 lỗ hổng bảo mật, đáng chú ý là các lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng.

2. Tăng cường giám sát và sẵn sàng các phương án xử lý khi phát hiện có dấu hiện bị khai thác, tấn công mạng; Đồng thời 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.

Trong quá trình triển khai, thực hiện có khó khăn, vướng mắc xin liên hệ Sở Y tế (qua Văn phòng Sở gặp ông Vũ Mạnh Thắng, số điện thoại 0988.202.102) để được trao đổi, hướng dẫn.

Nhận được Công văn này đề nghị lãnh đạo cơ quan, đơn vị quan tâm, thực hiện./.

Nơi nhận:
- Như trên;
- GĐ và các PGĐ Sở Y tế (để b/cáo);
- Trang Thông tin điện tử Sở Y tế;
- Trang Hồ sơ công việc;
- Lưu: VT, vmthang.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ Y TẾ
TỈNH KIÊN GIANG

Đỗ Thiện Tùng

Người ký: Sở Y tế
Email: syt@kiengiang.gov.vn
Cơ quan: Tỉnh Kiên Giang
Thời gian ký: 27.04.2023 16:32:39 +07:00

UBND TỈNH KIÊN GIANG
SỞ Y TẾ

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

PHỤ LỤC
Thông tin về lỗ hổng bảo mật trong sản phẩm Microsoft công bố tháng 04/2023
(Đính kèm theo Công văn số 1288 /SYT-VP ngày 27/4/2023 của Sở Y tế)

I. Các lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng:

- Lỗ hổng bảo mật **CVE-2023-28252** trong Windows Common Log File System Driver cho phép đối tượng tan 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**.

II. Thông tin các lỗ hổng bảo mật:

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-28252	- 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	- 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	- 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/CV-2023-23375 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28304

4	CVE-2013-3900	- 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 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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900
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/CV-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/CV-2023-28314

III. 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. Đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo tại mục II của phụ lục.

IV. Tài liệu tham khảo:

- https://msrc.microsoft.com/update-guide
- https://www.zerodayinitiative.com/blog/2023/4/11/the-april-2023-security- update-review

BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

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

Số: 349 /CNTT-YTĐT
V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 04/2023.

Hà Nội, ngày 20 tháng 04 năm 2023

Kính gửi:

- Vụ, Cục, Tổng cục, Văn phòng Bộ, Thanh tra Bộ;
- Các đơn vị trực thuộc Bộ Y tế;
- Các Sở Y tế.

Cục Công nghệ thông tin nhận được công văn số 554/CATTT-NCSC ngày 17/04/2023 của Cục An toàn thông tin về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 04/2023.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, Cục Công nghệ thông tin trân trọng đề nghị Quý đơn vị:

1. Kiểm tra, rà soát, xác định máy 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 (*tham khảo thông tin 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; đồng thời 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.

Trong trường hợp cần thiết, Quý Đơn vị liên hệ Trung tâm Dữ liệu y tế, Cục Công nghệ thông tin, Bộ Y tế (ThS. Hoàng Đăng Trị, điện thoại: 0987772483; Email: trihd.cntt@moh.gov.vn) để được hỗ trợ.

Trân trọng./.

Nơi nhận:
- Như trên;
- Trung tâm Dữ liệu y tế (để thực hiện);
- Lưu: VT, CNTT.

CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN
BỘ Y TẾ

Đỗ Trường Duy

BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

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

PHỤ LỤC I
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM MICROSOFT

(Kèm theo Công văn số 349 /CNTT-YTĐT ngày 20 /04 /2023 của Cục Công nghệ thông tin)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-28252	- 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	- 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	- 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	- 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 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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900
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. 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

https://www.zerodayinitiative.com/blog/2023/4/11/the-april-2023-security-update-review

UBND TỈNH KIÊN GIANG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số : 749 /STTTT-CĐS
V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 04/2023

Kiên Giang, ngày 19 tháng 4 năm 2023

Kính gửi:
- Văn phòng UBND tỉnh;
- Sở, ban, ngành cấp tỉnh;
- UBND các huyện, thành phố;
- UBND các xã, phường, thị trấn.

Sở Thông tin và Truyền thông nhận được Công văn số 554/CATTT-NCSC ngày 17/4/2023 của Cục An toàn thông tin về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 04/2023.

Theo đó, Microsoft vừa phát hành danh sách bản vá lỗi tháng 04/2023 với 97 lỗ hổng bảo mật, đáng chú ý là các lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng, như 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.

Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị, địa phương kiểm tra, rà soát các máy tính có sử dụng sản phẩm Microsoft để thực hiện vá lỗi các lỗ hổng theo hướng dẫn của Microsoft nhằm giảm thiểu nguy cơ bị tấn công. *(Chi tiết phụ lục kèm theo).*

Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, vui lòng liên hệ Phòng Chuyển đổi số - Sở Thông tin và Truyền thông, điện thoại: 02973.921678 hoặc 0918693113 (đ/c Nghĩa).

Trân trọng./.

Nơi nhận:
- Như trên;
- Trung tâm CNTTTT (thực hiện);
- Lưu: VT, CĐS (vbđt).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XHCN VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH KIÊN GIANG

Nguyễn Xuân Kiệm

PHỤ LỤC
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM CỦA MICROSOFT

(Kèm theo Công văn số 719 /STTTT-CĐS ngày 19 / 4/2023 của Sở Thông tin và Thông tin)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-28252	- 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	- 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	- 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	- 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 cơ quan, đơn vị, địa phương 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/2023/4/11/the-april-2023-security-update-review