UBND TỈNH NINH THUẬN
SỞ Y TẾ

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

Số: 1310 /SYT-VP

Ninh Thuận, ngày 29 tháng 3 năm 2023

V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 2, tháng 3 năm 2023.

Kính gửi: Các đơn vị trực thuộc.

Tiếp nhận Công văn số 303/STTTT-TTCNTT&TT; Công văn số 614/STTTT-TTCNTT&TT ngày 20/3/2023 của Sở Thông tin và Truyền thông về lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02 và tháng 3 năm 2023.

Microsoft đã phát hành danh sách bản vá tháng 2 và tháng 3 với 149 lỗ hổng bảo mật trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý các lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng, cụ thể như sau: *(1)* 04 lỗ hổng bảo mật CVE-2023-21529, CVE-2023-21710, CVE-2023-21707, CVE-2023-21706 trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa. Microsoft Exchange Server đã và đang là mục tiêu hàng đầu được các nhóm tấn công có chủ đích (APT) nhắm đến, các đối tượng tấn công khai thác triệt để. Vì vậy, các cơ quan, tổ chức cần đặc biệt chú ý cũng như có kế hoạch để khắc phục và tăng cường giám sát nhằm giảm thiểu và tránh nguy cơ bị tấn công thông qua các lỗ hổng này; *(2)* Lỗ hổng bảo mật CVE-2023-21716 trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa; *(3)* Lỗ hổng bảo mật CVE-2023-21715 trong Microsoft Publisher cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đang bị khai thác trong thực tế; *(4)* 02 lỗ hổng bảo mật CVE-2023-23376, CVE-2023-21812 trong Windows Common Log File System (CLFS) cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế*; (5)* 03 lỗ hổng bảo mật CVE-2023-21705, CVE-2023-21713, CVE-2023-21528 trong Microsoft SQL Server cho phép đối tượng tấn công thực thi mã từ xa; *(6)* Lỗ hổng bảo mật CVE-2023-21717 trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền; *(7)* Lỗ hổng bảo mật CVE-2023-23397 trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế; *(8)* Lỗ hổng bảo mật CVE-2023-24880 trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đang bị khai thác trong thực tế*; (9)* Lỗ hổng bảo mật CVE-2023-23392 trong HTTP Protocol Stack cho phép đối tượng

tấn công thực thi mã từ xa; *(10)* Lỗ hổng bảo mật CVE-2023-23415 trong Internet Control Message Protocol (ICMP) cho phép đối tượng tấn công thực thi mã từ xa; *(11)* Lỗ hổng bảo mật CVE-2023-23399 trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa; *(12)* Lỗ hổng bảo mật CVE-2023-23400 trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa.

(Thông tin chi tiết các lỗ hổng bảo mật có tại phụ lục kèm theo).

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Y tế yêu cầu các đơn vị thực hiện:

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.

3. Trong trường hợp cần được hỗ trợ các đơn vị liên hệ Trung tâm Giám sát an toàn, an ninh, thông tin mạng *(qua tổng đài điện thoại 1022 hoặc thư điện tử: ioc@ninhthuan.gov.vn)*.

Sở Y tế thông báo và yêu cầu các đơn vị triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Lãnh đạo Sở;
- Website Sở Y tế;
- Lưu: VT, VP.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ Y TẾ
TỈNH NINH THUẬN

Bùi Văn Kỳ

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM MICROSOFT
(Kèm theo Công văn số /SYT-VP ngày / /2023 của Sở Y tế)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-21529, CVE-2023-21710, CVE-2023-21707, CVE-2023-21706	- Điểm: CVSS: 8.8/7.2 (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-2023-21529 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21706 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21710 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21707
2	CVE-2023-21716	- Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hổng trong trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Word, Microsoft SharePoint.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21716
3	CVE-2023-21715	- Điểm: CVSS: 7.3 (cao) - Mô tả: lỗ hổng trong Microsoft Publisher cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft 365.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21715

4	CVE-2023-23376, CVE-2023-21812	- Điểm: CVSS: 7.8 (cao) - Mô tả: lỗ hổng trong Windows Common Log File System (CLFS) 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 10/11, Windows Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23376 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21812
5	CVE-2023-21705, CVE-2023-21713, CVE-2023-21528	- Điểm: CVSS: 8.8/7.8 (cao) - Mô tả: lỗ hổng trong Microsoft SQL Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: SQL Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21705 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21713 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21528
6	CVE-2023-21717	- Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Microsoft SharePoint.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21717
7	CVE-2023-23397	- Điểm: CVSS: 9.1 (nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Outlook 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: Microsoft Outlook, Microsoft Office.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397
8	CVE-2023-24880	- Điểm: CVSS: 5.4 (trung bình) - Mô tả: lỗ hổng trong	https://msrc.microsoft.com/update-guide/vulnerability/CVE-

		Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows Server, Windows 10/11.	2023-24880
9	CVE-2023-23392	- Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hổng trong HTTP Protocol Stack cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server, Windows 11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23392
10	CVE-2023-23415	- Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hổng trong Internet Control Message Protocol (ICMP) 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-2023-23415
11	CVE-2023-23399	- 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 Excel, Microsoft 365 .	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23399
12	CVE-2023-23400	- Điểm: CVSS: 7.2 (cao) - Mô tả: lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23400

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. 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/2023/2/14/the-february-2023-security-update-overview