UBND TỈNH NINH THUẬN
SỞ Y TẾ
Số: 1627 /SYT-KHNVTC

V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 04/2024.

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

Ninh Thuận, ngày 23 tháng 4 năm 2024

Kính gửi: Các đơn vị trực thuộc.

Tiếp nhận Công văn số 968/STTTT-TTCNTT&TT ngày 19/4/2024 của Sở Thông tin và Truyền thông về lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 4/2024.

Ngày 09/4/2024, Microsoft đã phát hành danh sách bản vá tháng 04 với 147 lỗ hổng an toàn thông tin trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý vào các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng sau: *(1)* Lỗ hổng an toàn thông tin CVE-2024-20678 trong Remote Procedure Call Runtime (RPC) cho phép đối tượng tấn công thực thi mã từ xa; *(2)* Lỗ hổng an toàn thông tin CVE-2024-29988 trong SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo vệ; *(3)* 03 lỗ hổng an toàn thông tin CVE-2024-21322, CVE-2024-21323, CVE-2024-29053 trong Microsoft Defender for IoT cho phép đối tượng tấn công thực thi mã từ xa; *(4)* Lỗ hổng an toàn thông tin CVE-2024-20670 trong Outlook for Windows làm lộ lọt NTML hash, cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing); *(5)* Lỗ hổng an toàn thông tin CVE-2024-26256 trong thư viện nguồn mở libarchive cho phép đối tượng tấn công thực thi mã từ xa; *(6)* Lỗ hổng an toàn thông tin CVE-2024-26257 trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa; *(7)* 07 lỗ hổng an toàn thông tin CVE-2024-26221, CVE-2024-26222, CVE-2024-26223, CVE-2024-26224, CVE-2024-26227, CVE-2024-26231, CVE-2024-26233 trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa; *(8)* Lỗ hổng an toàn thông tin CVE-2024-26234 trong Proxy Driver cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing).

(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, KHNVTC.

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 1627 /SYT-KHNVTC ngày 23 / 4/2024 của Sở Y tế)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-20678	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Remote Procedure Call Runtime (RPC) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20678
2	CVE-2024-29988	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29988
3	CVE-2024-21322 CVE-2024-21323 CVE-2024-29053	- Điểm: CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Defender for IoT cho phép đối tượng	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21322 https://msrc.microsoft.co

		tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Defender for IoT.	m/update-guide/vulnerability/CVE-2024-21323 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29053
4	CVE-2024-20670	- Điểm: CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng trong Outlook for Windows làm lộ lọt NTML hash, cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). - Ảnh hưởng: Outlook for Windows.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20670
5	CVE-2024-26256	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong thư viện nguồn mở libarchive cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 11; Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26256
6	CVE-2024-26257	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26257

		- Ảnh hưởng: Microsoft 365 Apps for Enterprise, Microsoft Office LTSC for Mac.	
7	CVE-2024-26221 CVE-2024-26222 CVE-2024-26223 CVE-2024-26224 CVE-2024-26227 CVE-2024-26231 CVE-2024-26233	- 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 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26221 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26222 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26223 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26224 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26227 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26231 https://msrc.microsoft.com/update-

			guide/vulnerability/CVE-2024-26233
8	CVE-2024-26234	- Điểm: CVSS: 6.7 (Cao) - Mô tả: Lỗ hổng trong Proxy Driver cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26234

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/2024/4/9/the-april-2024-security-updates-review