

V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 08/2024.

Kính gửi: Các đơn vị trực thuộc.

Tiếp nhận Công văn số 2438/STTTT-TTCNTTTT ngày 20/8/2024 của Sở Thông tin và Truyền thông về việc lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 8/2024.

Ngày 13/8/2024, Microsoft đã phát hành danh sách bản vá tháng 08 với 90 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-2024-38063 trong Windows TCP/IP cho phép đối tượng tấn công thực thi mã từ xa; (2) Lỗ hổng an toàn thông tin CVE-2024-38199 trong Windows Line Printer Daemon (LPD) Service cho phép đối tượng tấn công thực thi mã từ xa. Thông tin chi tiết về lỗ hổng đã được công bố công khai; (3) Lỗ hổng an toàn thông tin CVE-2024-38189 trong Microsoft Project cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng hiện đang bị khai thác trong thực tế; (4) 02 lỗ hổng an toàn thông tin CVE-2024-38218, CVE-2024-38219 trong Microsoft Edge cho phép đối tượng tấn công thực thi mã từ xa; (5) Lỗ hổng an toàn thông tin CVE-2024-38193 trong Windows Ancillary Function Driver for WinSock cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế; (6) Lỗ hổng an toàn thông tin CVE-2024-38107 trong Windows Power Dependency Coordinator cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế (*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*).

Yêu cầu Lãnh đạo các đơn vị tổ chức thực hiện an toàn và hiệu quả.

(*Gửi kèm theo Công văn số 2438/STTTT-TTCNTTTT ngày 20/8/2024 của Sở Thông tin và Truyền thông*)

Nơi nhận:

- Như trên;
- Lãnh đạo SYT;
- Các phòng của SYT;
- TTYT huyện, TP;
- Website SYT;
- Lưu: VT, KHNVTTC.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**



Bùi Văn Kỳ

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG
SẢN PHẨM MICROSOFT

(Kèm theo Công văn số /SYT-KHNVT ngày / /2024 của Sở Y tế)

1. Thông tin các lỗ hỏng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-38063	<ul style="list-style-type: none">- Điểm CVSS: 9.8 (Nghiêm trọng)- Mô tả: Lỗ hỏng trong Windows TCP/IP 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-2024-38063
2	CVE-2024-38199	<ul style="list-style-type: none">- Điểm CVSS: 9.8 (Cao)- Mô tả: Lỗ hỏng trong Windows Line Printer Daemon (LPD) Service cho phép đối tượng tấn công thực thi mã từ xa. Thông tin chi tiết về lỗ hỏng đã được công bố công khai.- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199
3	CVE-2024-38189	<ul style="list-style-type: none">- Điểm CVSS: 8.8 (Cao)- Mô tả: Lỗ hỏng trong Microsoft Project cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hỏng hiện đang bị khai thác trong thực tế.- Ảnh hưởng: Microsoft Project 2016, Microsoft Office 2019, Microsoft 365 Apps for Enterprise, Microsoft Office LTSC 2021.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38189
4	CVE-2024-38218 CVE-2024-38219	<ul style="list-style-type: none">- Điểm CVSS: 8.4 (Cao)- Mô tả: Lỗ hỏng trong Microsoft Edge cho phép đối tượng tấn công thực thi mã từ	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38218

		xa. - Ảnh hưởng: Microsoft Edge (Chromium-based).	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38219
5	CVE-2024-38193	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows Ancillary Function Driver for WinSock cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193
6	CVE-2024-38107	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows Power Dependency Coordinator cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107
7	CVE-2024-38170 CVE-2024-38172	- 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 365 Apps for Enterprise, Microsoft Office LTSC for Mac 2021.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38170 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38172
8	CVE-2024-38171	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft PowerPoint cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft PowerPoint 2016, Microsoft Office 2019, Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38171
9	CVE-2024-38178	- Điểm CVSS: 7.5 (Cao)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178

		<ul style="list-style-type: none"> - Mô tả: Lỗ hổng trong Scripting Engine cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022. 	com/update-guide/vulnerability/CVE-2024-38178
10	CVE-2024-38202	<ul style="list-style-type: none"> - Điểm CVSS: 7.3 (Cao) - Mô tả: Lỗ hổng trong Windows Update Stack cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38202
11	CVE-2024-38106	<ul style="list-style-type: none"> - Điểm CVSS: 7.0 (Cao) - Mô tả: Lỗ hổng trong Windows Kernel cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106
12	CVE-2024-21302	<ul style="list-style-type: none"> - Điểm CVSS: 6.7 (Cao) - Mô tả: Lỗ hổng trong Windows Secure Kernel Mode cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21302
13	CVE-2024-38173	<ul style="list-style-type: none"> - Điểm CVSS: 6.7 (Cao) - Mô tả: Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Outlook 2016, Microsoft 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38173

		Office 2019, Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise.	
14	CVE-2024-38200	<ul style="list-style-type: none"> - Điểm CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: Microsoft Office 2016, 2019, Microsoft 365 Apps for Enterprise, Microsoft Office LTSC 2021. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38200
15	CVE-2024-38213	<ul style="list-style-type: none"> - Điểm CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng trong Windows Mark of the Web Security cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213

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/2024/8/13/the-august-2024-security-update-review>