ỦY BAN NHÂN DÂN **HUYỆN NGHĨA HÀNH**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 2096 /UBND V/v cảnh báo lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 8/2024	*Nghĩa Hành, ngày 23 tháng 8 năm 2024*

Kính gửi:

- Các cơ quan, đơn vị; Hội, đoàn thể huyện;
- UBND các xã, thị trấn;
- Công an huyện.

Theo cảnh báo của Sở Thông tin và Truyền thông tại Công văn số 1887/STTTT-BCVT&CNTT ngày 19/8/2024 về lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 8/2024, Ủy ban nhân dân huyện yêu cầu lãnh đạo các cơ quan, đơn vị chỉ đạo thực hiện một số biện pháp sau để hạn chế các rủi ro về nguy cơ mất an toàn thông tin, cụ thể:

1. Kiểm tra, rà soát máy chủ, máy trạm có sử dụng hệ điều hành Windows để phát hiện và xử lý kịp thời các máy chủ có khả năng bị ảnh hưởng bởi các lỗ hổng bảo mật 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.

(Tham khảo thông tin lỗ hổng và cách khắc phục tại Phụ lục Thông tin về lỗ hổng bảo mật kèm theo Công văn này)

2. Khi phát hiện các hệ thống có biểu hiện bị khai thác, tấn công mạng, triển khai ngay các biện pháp xử lý ngăn chặn tấn công trên hệ thống và thông báo về UBND huyện (qua Phòng Văn hóa và Thông tin) để tổng hợp báo cáo Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi có các biện pháp hỗ trợ, xử lý kịp thời.

Yêu cầu lãnh đạo các cơ quan, đơn vị quan tâm chỉ đạo thực hiện./.

***Nơi nhận*:**
- Như trên;
- Sở Thông tin và Truyền thông (báo cáo);
- CT, các PCT UBND huyện;
- Văn phòng HĐND&UBND huyện;
- Lưu: VT, PVHTT.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Ngọc Tuấn

PHỤ LỤC
HƯỚNG DẪN VỀ CÁC LỖ HỔNG AN TOÀN THÔNG TIN TRONG SẢN PHẨM MICROSOFT
(Kèm theo Công văn số 2096 /UBND ngày 23 /8/2024 của Ủy ban nhân dân huyện Nghĩa Hành)

1. Thông tin các lỗ hổng an toàn thông tin

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-38063	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng 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	- Điểm CVSS: 9.8 (Cao) - Mô tả: Lỗ hổng 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. - 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	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Project cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Project	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38189

STT	CVE	Mô tả	Link tham khảo
		2016, Microsoft Office 2019, Microsoft 365 Apps for Enterprise, Microsoft Office LTSC 2021.	
4	CVE-2024-38218 CVE-2024-38219	- Điểm CVSS: 8.4 (Cao) - Mô tả: Lỗ hổng trong Microsoft Edge cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Edge (Chromium-based).	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38218 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	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107

STT	CVE	Mô tả	Link tham khảo
		2012, 2016, 2019, 2022.	
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) - 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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178

STT	CVE	Mô tả	Link tham khảo
10	CVE-2024-38202	- 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	- 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	- 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

STT	CVE	Mô tả	Link tham khảo
13	CVE-2024-38173	- 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 Office 2019, Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38173
14	CVE-2024-38200	- 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	- 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 an toàn thông tin 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