

2	CVE-2024-38199	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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 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 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	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗi hỏng trong Windows Ancillary Function Driver for WinSock cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗi hỏng 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	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗi hỏng trong Windows Power Dependency Coordinator cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗi hỏng 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	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗi hỏng 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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
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 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	<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

- **Đánh giá mức độ:** Đánh giá sơ bộ từ các chuyên gia bảo mật, lỗ hổng này ảnh hưởng đến nhiều thiết bị trên toàn cầu trong đó có cả Việt Nam. Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) đánh giá khả năng các mã khai thác của các lỗ hổng này sẽ sớm được công khai trên Internet trong thời gian sắp tới.

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. Nguồn tham khảo:

<https://msrc.microsoft.com/update-guide/>

<https://www.zerodayinitiative.com/blog/2024/8/13/the-august-2024-security-update-review>