UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1625 /STTTT-TTGSĐH
V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 08/2024

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

Tây Ninh, ngày 20 tháng 8 năm 2024

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các cơ quan tham mưu, giúp việc Tỉnh ủy;
- Mặt trận Tổ quốc và các Đoàn thể chính trị - xã hội;
- Các Sở, ban, ngành tỉnh;
- Các đơn vị ngành dọc;
- Các huyện, thị, thành ủy trực thuộc Tỉnh ủy;
- UBND các huyện, thị xã, thành phố;
- UBND các xã, phường, thị trấn.

Thực hiện theo Công văn số 1667/CATTT-NCSC ngày 19/8/2024 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 08/2024 ***(Thông tin chi tiết phụ lục kèm theo)***.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin cho người dùng, đơn vị và toàn bộ hệ thống của tỉnh, Sở Thông tin và Truyền thông đề nghị các đơn vị, địa phương thực hiện gấp các công việc cụ thể như sau:

1. Kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows và phần mềm có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời theo hướng dẫn tại phụ lục để tránh nguy cơ bị tấn công.

2. Tăng cường kiểm tra, giám sát hệ thống mạng của đơn vị, địa phương, khi có phát hiện hoạt động tấn công mạng, đề nghị liên hệ Sở Thông tin và Truyền thông để phối hợp xử lý kịp thời.

Thông tin liên quan đề nghị liên hệ Ông Đào Quang Phúc - Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung; Điện thoại: 0937.117.128.

Trân trọng./.

Nơi nhận:
- Như trên;
- BGĐ Sở (b/c);
- P.CNTTBCVT;
- Lưu: VT, TTGSĐH.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TÂY NINH

Nguyễn Trung Hiếu

PHỤ LỤC
Thông tin các lỗ hổng nghiêm trọng trong các sản phẩm Microsoft công bố tháng 08/2024

1.Thông tin lỗ hổng bảo mật

- Mô tả:

- Lỗ hổng an toàn thông tin **CVE-2024-38063** trong Windows TCP/IP cho phép đối tượng tấn công thực thi mã từ xa.

- 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.

- 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.

- 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.

- 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.

- 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.

- Ảnh hưởng:

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 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	- 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 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) - 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	- 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
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

- 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