

UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: /STTTT-TTGSĐH

V/v lỗ hổng an toàn thông tin ảnh hưởng cao và
nghiêm trọng trong các sản phẩm Microsoft công
bố tháng 05/2024

Tây Ninh, ngày tháng 05 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 884/CATTT-NCSC 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 05/2024 (**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**

PHỤ LỤC
Thông tin các lỗ hổng nghiêm trọng trong các sản phẩm
Microsoft công bố tháng 05/2024

1. Thông tin lỗ hổng bảo mật

- Mô tả:

- Lỗ hổng an toàn thông tin **CVE-2024-30040** trong Windows MSHTML Platform cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2024-30044** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- **03** lỗ hổng an toàn thông tin **CVE-2024-30051, CVE-2024-30032, CVE-2024-30035** trong Windows DWM Core Library cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2024-30042** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-30033** trong Windows Search Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.

- Lỗ hổng an toàn thông tin **CVE-2024-30043** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện tấn công XXE.

- Ảnh hưởng:

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-30040	<p>- Điểm: CVSS: 8.8 (Cao)</p> <p>- Mô tả: Lỗ hổng trong Windows MSHTML Platform cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế.</p> <p>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022.</p>	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30040

2	CVE-2024-30044	<ul style="list-style-type: none"> - Điểm: CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30044
3	<p>CVE-2024-30051 CVE-2024-30032 CVE-2024-30035</p>	<ul style="list-style-type: none"> - Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows DWM Core Library cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022. 	<p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30051 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30032 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30035</p>
4	CVE-2024-30042	<ul style="list-style-type: none"> - 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 Excel, Office Online Server, Microsoft 365 Apps, Microsoft Office LTSC. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30042

5	CVE-2024-30033	<ul style="list-style-type: none"> - Điểm: CVSS: 7.0 (Cao) - Mô tả: Lỗ hổng trong Windows Search Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30033
6	CVE-2024-30043	<ul style="list-style-type: none"> - Điểm: CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện tấn công XXE. - Ảnh hưởng: Microsoft SharePoint Server. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30043

- 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/2024/5/14/the-may-2024-security-update-review>