

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 03/2024

Tây Ninh, ngày tháng 03 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 364/CATTT-NCSC của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 03/2024 (**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.

GIÁM ĐỐC

PHỤ LỤC
Thông tin các lỗ hổng an toàn thông tin nghiêm trọng
trong các sản phẩm Microsoft công bố tháng 03/2024

1. Thông tin lỗ hổng bảo mật

- Mô tả:

- Lỗ hổng an toàn thông tin **CVE-2024-26198** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-21407** trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-21408** trong Windows Hyper-V cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ (DoS).

- Lỗ hổng an toàn thông tin **CVE-2024-21334** trong Open Management Infrastructure (OMI) cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-21426** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-21411** trong Skype for Consumer cho phép đối tượng tấn công thực thi mã từ xa.

- Ảnh hưởng:

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-26198	<ul style="list-style-type: none">- Điểm: CVSS: 8.8 (Cao)- Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.- Ảnh hưởng: Microsoft Exchange Server 2016, 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26198
2	CVE-2024-21407	<ul style="list-style-type: none">- Điểm: CVSS: 8.1 (Nghiêm trọng)- Mô tả: Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21407

		- Ảnh hưởng: Windows 10, Windows 11; Windows Server 2012, 2012 R2, 2016, 2019, 2022.	
3	CVE-2024-21408	- Điểm: CVSS: 5.5 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ (DoS). - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21408
4	CVE-2024-21334	- Điểm: CVSS: 9.8 (Cao) - Mô tả: Lỗ hổng trong Open Management Infrastructure (OMI) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: OMI; System Center Operations Manager (SCOM) 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21334
5	CVE-2024-21426	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server 2019; Microsoft	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21426

		SharePoint Server Subscription Edition.	
6	CVE-2024-21411	<ul style="list-style-type: none"> - Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Skype for Consumer cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Skype for Consumer. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21411

- **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/2024/3/12/the-march-2024-security-update-review>