

Số: /STTTT-BCVTCNTT

Lai Châu, ngày tháng năm 2024

V/v Lỗ hổng an toàn thông tin ảnh hưởng
cao và nghiêm trọng trong các sản phẩm
Microsoft công bố tháng 03/2024

Kính gửi:

- Các Sở, Ban, Ngành tỉnh;
- UBND các huyện, thành phố.

Ngày 12/3/2024, Microsoft đã phát hành danh sách bản vá tháng 03 với 59 lỗ hổng an toàn thông tin trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý vào các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng sau:

- 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.

(Thông tin chi tiết các lỗ hổng bảo mật xin xem tại phụ lục kèm theo)

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị

tấn công (*tham khảo thông tin tại phụ lục kèm theo*).

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

3. Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin để được hỗ trợ: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ais@mic.gov.vn hoặc Phòng Bru chính - Viễn thông - Công nghệ thông tin, số điện thoại: 02133798798.

Trên đây là cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 03/2024, kính đề nghị Quý cơ quan quan tâm thực hiện./.

Nơi nhận:

- Như trên;
- Lưu: VT, BCVTCNTT.

GIÁM ĐỐC

Nguyễn Minh Hiệu

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT
TRONG SẢN PHẨM CỦA MICROSOFT

(Kèm theo Công văn số /STTTT-BCVTCNTT ngày / /2024 của Sở
Thông tin và Truyền thông)

1. Thông tin các lỗ hổng an toàn thông tin

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. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2012, 2012 R2, 2016, 2019, 2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21407
3	CVE-2024-21408	<ul style="list-style-type: none"> - 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; 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21408

		Windows Server 2016, 2019, 2022.	
4	CVE-2024-21334	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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 SharePoint Server Subscription Edition. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21426
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

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