

Số: /STTTT-CĐS

Kiên Giang, 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 01/2024

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng UBND tỉnh;
- Sở, ban, ngành cấp tỉnh;
- UBND các huyện, thành phố;
- Phòng Văn hóa - Thông tin các huyện, thành phố.

Sở Thông tin và Truyền thông Kiên Giang nhận được Công văn số 66/CATTT-NCSC ngày 17/01/2024 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2024.

Theo đó ngày 09/01/2024, Microsoft đã phát hành danh sách bản vá tháng 01 với 49 lỗ hổng an toàn thông tin trong các sản phẩm của Microsoft. Bản phát hành tháng 01 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-2024-20674** trong Windows Kerberos cho phép đối tượng tấn công vượt qua cơ chế bảo vệ để thực hiện tấn công giả mạo.

- Lỗ hổng an toàn thông tin **CVE-2024-21318** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-20677** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-20700** trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa.

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

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh, góp phần bảo đảm an toàn cho không gian mạng Việt Nam. Sở Thông tin và Truyền thông Kiên Giang khuyến nghị các cơ quan, đơn vị thực hiện một số biện pháp sau:

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 sau:

- Cục An toàn thông tin - Bộ Thông tin và Truyền thông: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ncsc@ais.gov.vn.

- Hoặc Phòng Chuyên đổi số - Sở Thông tin và Truyền thông Kiên Giang, điện thoại: 0297.3921678, 0918767498 (đ/c Nghi), thư điện tử: ttnghi.sttt@kiengiang.gov.vn.

Trân trọng./.

Nơi nhận:

- Như trên;
- Trung tâm CNTTTT (thực hiện);
- Lưu: VT, CDS, ttnghi.

GIÁM ĐỐC

Võ Minh Trung

PHỤ LỤC
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT
TRONG SẢN PHẨM CỦA MICROSOFT
(Kèm theo Công văn số /STTTT-CĐS ngày / 01 /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-2024-20674	<ul style="list-style-type: none">- Điểm: CVSS: 9.0 (Nghiêm trọng)- Mô tả: Lỗ hổng trong Windows Kerberos cho phép đối tượng tấn công vượt qua cơ chế bảo vệ để thực hiện tấn công giả mạo.- Ảnh hưởng: Windows 10, Windows 11; Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20674
2	CVE-2024-21318	<ul style="list-style-type: none">- Điểm: CVSS: 8.8 (Cao)- Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.- Ảnh hưởng: Microsoft SharePoint Server 2016, 2019; Microsoft SharePoint Server Subscription Edition.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21318
3	CVE-2024-20677	<ul style="list-style-type: none">- Điểm: CVSS: 7.8 (Cao)- Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.- Ảnh hưởng: Microsoft Office 2019; Microsoft Office LTSC; Microsoft 365 Apps.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20677

4	CVE-2024-20700	<ul style="list-style-type: none"> - Điểm: CVSS: 7.5 (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 2019, 2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20700
---	-----------------------	--	---

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 cơ quan, đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại “**Link cập nhật tham khảo**” mục 1 của bảng Phụ lục này.

3. Tài liệu tham khảo

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

<https://www.zerodayinitiative.com/blog/2024/1/9/the-january-2024-security-update-review>