

Số: /STTTT-CNTT

Đắk Lắk, ngày tháng 6 năm 2024

V/v hướng dẫn khắc phục lỗ hổng bảo mật
ảnh hưởng mức cao và nghiêm trọng trong
các sản phẩm Microsoft công bố tháng 6/2024

Kính gửi:

- Các sở, ban, ngành và đoàn thể của tỉnh;
- UBND các huyện, thị xã, thành phố;
- Trung tâm Giám sát, điều hành đô thị thông minh.

Ngày 11/6/2024, Microsoft đã phát hành danh sách bản vá tháng 6/2024 với 49 lỗ hổng bảo mật trong các sản phẩm của mình. Bản phát hành tháng này, đặc biệt đáng chú ý các lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng (*Có Phụ lục gửi kèm theo*).

Thực hiện Công văn số 1096/CATTT-NCSC ngày 14/6/2024 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc lỗ hổng an toàn thông tin ảnh hưởng nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2024. Đồng thời, nhằm đảm bảo an toàn thông tin cho các hệ thống thông tin của cơ quan, đơn vị trên địa bàn tỉnh, Sở Thông tin và Truyền thông khuyến nghị các cơ quan, đơn vị triển khai các nội dung 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 về lỗ hổng bảo mật tại Phụ lục gửi 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 được hỗ trợ, các cơ quan, đơn vị liên hệ đầu mối hỗ trợ của Cục An toàn thông tin và Sở 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.

- Trung tâm Giám sát, điều hành đô thị thông minh: Đồng chí Lê Xuân Quang, Phó Giám đốc Trung tâm, điện thoại 0975.001.578; thư điện tử: quanglx@tttt.daklak.gov.vn.

Nhận được Công văn này, Sở Thông tin và Truyền thông kính đề nghị các cơ quan, đơn vị quan tâm, triển khai thực hiện./.

Nơi nhận:

- Như trên;
- UBND tỉnh (b/c);
- Cục An toàn thông tin (b/c);
- Lãnh đạo Sở;
- Trung tâm IOC;
- Lưu: VT, CNTT.

GIÁM ĐỐC

Trương Hoài Anh

PHỤ LỤC

Thông tin về các lỗ hổng an toàn thông tin trong các sản phẩm Microsoft

(Kèm theo Công văn số: /STTTT-CNTT ngày / 6 /2024
của Sở Thông tin và Truyền thông tỉnh Đắk Lắk)

1. Thông tin các lỗ hổng về an toàn thông tin

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-30080	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Message Queuing (MSMQ) 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-2024-30080
2	CVE-2024-30103	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Outlook 2016, 2019, Microsoft 365 Apps for Enterprise, Microsoft Office LTSC 2021.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30103
3	CVE-2024-30078	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Windows Wi-Fi Driver 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-2024-30078
4	CVE-2024-30101 CVE-2024-30102 CVE-2024-30104	- 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 Outlook 2016, 2019, Microsoft 365 Apps for Enterprise, Microsoft Office LTSC 2021.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30101 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30102 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30104

5	CVE-2024-30100	- 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 Server 2019, Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server Subscription Edition.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30100
---	----------------	--	---

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/2024/6/11/the-june-2024-security-update-review>