UBND TỈNH NAM ĐỊNH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số:627 /STTTT-CĐS
V/v kiểm tra, rà soát và khắc phục lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2024

Nam Định, ngày 17 tháng 6 năm 2024

Kính gửi:
- Các sở, ban, ngành của tỉnh;
- UBND các huyện, thành phố;
- VNPT Nam Định;
- Viettel Nam Định.

Căn cứ Văn bản số 1096/CATTT-NCSC ngày 14/6/2024 của Cục An toàn thông tin về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 06/2024.

Theo đó, ngày 11/6/2024, Microsoft đã phát hành danh sách bản vá tháng 06 với 49 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-2024-30080 trong Microsoft Message Queuing (MSMQ) cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin CVE-2024-30103 trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin CVE-2024-30078 trong Windows Wi-Fi Driver cho phép đối tượng tấn công thực thi mã từ xa.

- 03 lỗ hổng an toàn thông tin CVE-2024-30101, CVE-2024-30102, CVE-2024-30104 trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin CVE-2024-30100 trong Microsoft SharePoint Server 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, doanh nghiệp trên địa bàn tỉnh, Sở Thông tin và Truyền thông đề nghị các sở, ban, ngành của tỉnh; UBND các huyện, thành phố và VNPT Nam Định, Viettel Nam Định phối hợp triển khai thực hiện một số nội dung sau:

1. Đề nghị các sở, ban, ngành của tỉnh; UBND các huyện, thành phố:

- Kiểm tra, rà soát và xác định máy chủ, máy trạm 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).

- Chỉ đạo, hướng dẫn, hỗ trợ các đơn vị trực thuộc và UBND các xã, phường, thị trấn tổ chức triển khai thực hiện nội dung trên.

- Tăng cường giám sát và kịp thời thông báo về Sở Thông tin và Truyền thông khi phát hiện có dấu hiệu bị khai thác, tấn công mạng.

2. Đề nghị VNPT Nam Định, Viettel Nam Định thực hiện việc rà soát, kiểm tra, cập nhật bản vá cho máy tính, thiết bị trong hệ thống thông tin đang cung cấp các dịch vụ, phần mềm cho các cơ quan nhà nước trên địa bàn tỉnh.

3. Yêu cầu Trung tâm Chuyển đổi số và Truyền thông:

- Thực hiện rà soát, kiểm tra; cập nhật bản vá bảo mật cho các máy bị ảnh hưởng đối với các máy tính, thiết bị tại Trung tâm Tích hợp dữ liệu của tỉnh.

- Làm đầu mối hỗ trợ, hướng dẫn các sở, ban, ngành của tỉnh; UBND các huyện, thành phố xử lý, khắc phục lỗ hổng.

- Chủ động triển khai các giải pháp và phối hợp với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin kịp thời xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng, đảm bảo an toàn thông tin tại Trung tâm Tích hợp dữ liệu của tỉnh.

Sở Thông tin và Truyền thông đề nghị các Sở, ban, ngành của tỉnh; UBND các huyện, thành phố và VNPT Nam Định, Viettel Nam Định quan tâm phối hợp triển khai thực hiện.

Thông tin liên hệ: Đầu mối hỗ trợ kỹ thuật: ông Trần Tuấn Anh, Kỹ sư Trung tâm Chuyển đổi số và Truyền thông (số điện thoại: 0376805976, email: trantuananh.stt@namdinh.gov.vn); Đầu mối tổng hợp: ông Phạm Văn An, Chuyên viên Phòng Chuyển đổi số (điện thoại: 0949268749, email: phamvanan.stt@namdinh.gov.vn).

Trân trọng./.

Nơi nhận:
- Như trên;
- Phòng VHTT các huyện, TP;
- Trung tâm VHTT&TT các huyện, TP;
- Trung tâm CĐS&TT (để thực hiện);
- Lưu: VT, CĐS (anpv).

GIÁM ĐỐC

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH NAM ĐỊNH

Vũ Trọng Quế

Phụ lục

Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft

(Kèm theo Văn bản số .../STTTT-CĐS ngày .../6/2024 của Sở TT&TT)

1. Thông tin các lỗ hổng bảo mật

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