BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Số: 241 /TTCNTT-HTATTT

V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 05/2024

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

Hà Nội, ngày 21 tháng 05 năm 2024

Kính gửi: Các đơn vị trực thuộc Bộ
(Danh sách kèm theo)

Ngày 14/05/2024, Microsoft đã phát hành danh sách bản vá tháng 05 với 59 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 trên máy tính người dùng và hệ thống thông tin như sau:

- Lỗ hổng an toàn thông tin **CVE-2024-30040** trong Windows MSHTML Platform cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2024-30044** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- 03 lỗ hổng an toàn thông tin **CVE-2024-30051, CVE-2024-30032, CVE-2024-30035** trong Windows DWM Core Library cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2024-30042** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-30033** trong Windows Search Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.

- Lỗ hổng an toàn thông tin **CVE-2024-30043** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện tấn công XXE.

Thông tin chi tiết các lỗ hổng an toàn thông tin, mức ảnh hưởng trên các sản phẩm xem tại Phụ lục kèm theo.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị và người sử dụng, Trung tâm Công nghệ thông tin khuyến nghị Quý đơn vị/cá nhân thực hiện:

1. Kiểm tra, rà soát, xác định máy 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.

Thông tin liên hệ: Anh Vũ Xuân Phương, Phòng Hạ tầng và an toàn thông tin, 113 Trần Duy Hưng, Trung Hòa, Cầu Giấy, Hà Nội; số điện thoại: 0941202428; địa chỉ thư điện tử: vxphuong@most.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Giám đốc (để b/c);
- Lưu: VT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Ngô Minh Phước

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM MICROSOFT
(Kèm theo Công văn số 241 /TTCNTT-HTATTT ngày21 / 05 /2024 của Trung tâm Công nghệ thông tin)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-30040	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Windows MSHTML Platform cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: **Máy tính** cài đặt Windows 10, Windows 11; **Hệ thống** cài đặt Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30040
2	CVE-2024-30044	- Điểm: CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: **Hệ thống** cài đặt Microsoft SharePoint Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30044
3	CVE-2024-30051 CVE-2024-30032 CVE-2024-30035	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows DWM Core Library cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: **Máy tính** cài đặt Windows 10, Windows 11; **Hệ thống** cài đặt Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30051 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30032 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30035

4	CVE-2024-30042	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: **Máy tính, hệ thống** cài đặt Microsoft Excel, Office Online Server, Microsoft 365 Apps, Microsoft Office LTSC.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30042
5	CVE-2024-30033	- Điểm: CVSS: 7.0 (Cao) - Mô tả: Lỗ hổng trong Windows Search Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: **Máy tính** cài đặt Windows 10, Windows 11; **Hệ thống** cài đặt Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30033
6	CVE-2024-30043	- Điểm: CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện tấn công XXE. - Ảnh hưởng: **Hệ thống** cài đặt Microsoft SharePoint Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30043

2. Hướng dẫn khắc phục

Biện pháp khuyến cáo để khắc phục là cập nhật bản vá cho các lỗ hổng bảo mật nêu trên theo hướng dẫn của hãng. Quý đơn vị/cá nhân tham khảo các bản cập nhật phù hợp cho các sản phẩm (trong mục Security Updates) đang sử dụng tại link nguồn tham khảo tại mục 1 của phụ lục.

Trên máy tính người dùng có thể thiết lập chế độ tự động tải các bản cập nhật như sau:

- Cập nhật hệ điều hành Windows theo hướng dẫn sau (có thể thiết lập các chế độ cập nhật trong mục cài đặt nâng cao “Advanced options”):

https://support.microsoft.com/vi-vn/windows/t%E1%BA%A3i-b%E1%BA%A3n-c%E1%BA%ADp-nh%E1%BA%ADt-windows-m%E1%BB%9Bi-nh%E1%BA%A5t-7d20e88c-0568-483a-37bc-c3885390d212#WindowsVersion=Windows_11

- Đối với các sản phẩm khác của Microsoft có thể thiết lập chế độ tự động cập nhật cùng với các bản cập nhật Windows theo hướng dẫn sau:

https://support.microsoft.com/vi-vn/office/c%E1%BA%ADp-nh%E1%BA%ADt-office-v%E1%BB%9Bi-microsoft-update-f59d3f9d-bd5d-4d3b-a08e-1dd659cf5282

3. Tài liệu tham khảo

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

https://www.zerodayinitiative.com/blog/2024/5/14/the-may-2024-security-update-review

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số 241 /TTCNTT-HTATTT ngày 21 /05/2024 của Trung tâm Công nghệ thông tin)

TT	Tên đơn vị
1.	Vụ Khoa học Xã hội, Nhân văn và Tự nhiên
2.	Vụ Khoa học và Công nghệ các ngành kinh tế - kỹ thuật
3.	Vụ Đánh giá, Thẩm định và Giám định công nghệ
4.	Vụ Công nghệ cao
5.	Vụ Năng lượng nguyên tử
6.	Vụ Ứng dụng công nghệ và tiến bộ kỹ thuật
7.	Vụ Kế hoạch -Tài chính
8.	Vụ Pháp chế
9.	Vụ Tổ chức cán bộ
10.	Vụ Hợp tác quốc tế
11.	Văn phòng Bộ
12.	Thanh tra Bộ
13.	Cục Phát triển công nghệ và Đổi mới sáng tạo.
14.	Cục Thông tin khoa học và công nghệ quốc gia
15.	Cục Phát triển thị trường và doanh nghiệp khoa học và công nghệ
16.	Cục An toàn bức xạ và hạt nhân
17.	Cục Sở hữu trí tuệ
18.	Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia
19.	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
20.	Viện Khoa học và công nghệ Việt Nam - Hàn Quốc (VKIST)
21.	Viện Nghiên cứu sáng chế và Khai thác công nghệ
22.	Viện Năng lượng nguyên tử Việt Nam
23.	Viện Ứng dụng công nghệ
24.	Viện Đánh giá khoa học và Định giá công nghệ
25.	Viện Khoa học sở hữu trí tuệ
26.	Viện Nghiên cứu và Phát triển Vùng
27.	Văn phòng các Chương trình trọng điểm cấp nhà nước
28.	Văn phòng Công nhận chất lượng
29.	Văn phòng Đăng ký hoạt động khoa học và công nghệ
30.	Văn phòng các Chương trình khoa học và công nghệ quốc gia
31.	Báo VnExpress

32.	Tạp chí Khoa học và Công nghệ Việt Nam
33.	Nhà xuất bản Khoa học và Kỹ thuật
34.	Quỹ Phát triển khoa học và công nghệ quốc gia
35.	Quỹ Đổi mới công nghệ quốc gia
36.	Trung tâm Nghiên cứu và Phát triển truyền thông khoa học và công nghệ
37.	Trung tâm Nghiên cứu và Phát triển hội nhập khoa học và công nghệ quốc tế
38.	Trung tâm Công nghệ thông tin
39.	Cổng thông tin điện tử của Bộ (để đăng tải)