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

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

Số: 264/TTCNTT-KTHT
V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 07/2023

Hà Nội, ngày 21 tháng 07 năm 2023

Kính gửi: Các đơn vị trực thuộc Bộ

Ngày 11/07/2023, Microsoft đã phát hành danh sách bản vá tháng 07 với 130 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 sau:

- 02 lỗ hổng bảo mật CVE-2023-33160, CVE-2023-33134 trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

Trong thời gian vừa qua, Trung tâm công nghệ thông tin đã phát hành các văn bản cảnh báo diện rộng về các lỗ hổng ảnh hưởng đến Microsoft SharePoint Server. Điều này cho thấy, Microsoft SharePoint Server vẫn luôn là mục tiêu hàng đầu được các nhóm tấn công có chủ đích (APT) nhắm đến. Vì vậy, để đảm bảo an toàn thông tin cho hệ thống của các đơn vị, Trung tâm công nghệ thông tin đề nghị Quý Đơn vị rà soát lỗ hổng liên quan đến Microsoft SharePoint Server để phát hiện và có phương án xử lý kịp thời, đồng thời tăng cường giám sát nhằm giảm thiểu nguy cơ bị tấn công thông qua các lỗ hổng này.

- Lỗ hổng bảo mật CVE-2023-36884 trong Office và Windows cho phép đối tượng tấn công thực thi mã từ xa khi người dùng mở tệp tài liệu của Microsoft Office do đối tượng tấn công tạo ra. Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật CVE-2023-35311 trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật CVE-2023-36874 trong Windows Error Reporting Service cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật CVE-2023-32046 trong Windows MSHTML cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật CVE-2023-32049 trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đang bị khai thác trong thực tế.

- 02 lỗ hổng bảo mật CVE-2023-32057, CVE-2023-35309 trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa.

Thông tin chi tiết các lỗ hổng có tại Phụ lục kèm theo.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý Đơn vị, Trung tâm Công nghệ thông tin 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.

Trong trường hợp cần thiết, Quý Đơn vị liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, số điện thoại 024.39439060, thư điện tử phongktht@most.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Giám đốc (để b/c);
- Cổng thông tin điện tử Bộ KH&CN;
- Lưu: VT, KTHT.

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 AN TOÀN THÔNG TIN TRONG SẢN PHẨM CỦA MICROSOFT

(Kèm theo Công văn số 264 /TTCNTT-KTHT ngày 21 /07 /2023 của Trung tâm Công nghệ thông tin)

1. Thông tin các lỗ hổng an toàn thông tin

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-33160 CVE-2023-33134	- 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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33160 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33134
2	CVE-2023-36884	- Điểm: CVSS: 8.3 (Cao) - Mô tả: lỗ hổng trong Office và Windows HTML cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, 11, Windows Server, Microsoft Office.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884
3	CVE-2023-35311	- Điểm: CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). - Ảnh hưởng: Microsoft 365, Microsoft Office, Microsoft Outlook.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35311
4	CVE-2023-36874	- Điểm: CVSS: 7.8 (Cao) - Mô tả: lỗ hổng trong Windows Error Reporting Service cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36874

		Server, Windows 10/11.	
5	CVE-2023-32046	- Điểm: CVSS: 7.8 (Cao) - Mô tả: lỗ hổng trong Windows MSHTML cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046
6	CVE-2023-32049	- Điểm: CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32049
7	CVE-2023-32057 CVE-2023-35309	- Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32057 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35309

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/2023/7/10/the-july-2023-security-update-review

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số 264 /TTCNTT-KTHT ngày21 /07 /2023 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	Vụ Thi đua khen thưởng
12	Văn phòng Bộ
13	Thanh tra Bộ
14	Cục Công tác phía Nam
15	Cục Phát triển công nghệ và Đổi mới sáng tạo
16	Cục Thông tin khoa học và công nghệ quốc gia
17	Cục Phát triển thị trường và doanh nghiệp khoa học và công nghệ
18	Cục An toàn bức xạ và hạt nhân
19	Cục Sở hữu trí tuệ
20	Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia
21	Ban quản lý Khu Công nghệ cao Hòa Lạc
22	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
23	Viện Khoa học và công nghệ Việt Nam - Hàn Quốc (VKIST)
24	Viện Nghiên cứu sáng chế và Khai thác công nghệ
25	Viện Năng lượng nguyên tử Việt Nam
26	Viện Ứng dụng công nghệ
27	Viện Đánh giá khoa học và Định giá công nghệ
28	Viện Khoa học sở hữu trí tuệ
29	Viện Nghiên cứu và Phát triển Vùng
30	Văn phòng các Chương trình trọng điểm cấp nhà nước

31	Văn phòng Công nhận chất lượng
32	Văn phòng Đăng ký hoạt động khoa học và công nghệ
33	Văn phòng các Chương trình khoa học và công nghệ quốc gia
34	Báo điện tử Tin nhanh Việt Nam (VnExpress)
35	Tạp chí Khoa học và Công nghệ Việt Nam
36	Nhà xuất bản Khoa học và Kỹ thuật
37	Quỹ Phát triển khoa học và công nghệ quốc gia
38	Quỹ Đổi mới công nghệ quốc gia
39	Trung tâm Nghiên cứu và Phát triển truyền thông khoa học và công nghệ
40	Trung tâm Nghiên cứu và Phát triển hội nhập khoa học và công nghệ quốc tế
41	Trung tâm Công nghệ thông tin