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

Số: 21 /TTCNTT-KTHT
V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2023

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

Hà Nội, ngày 13 tháng 01 năm 2023

Kính gửi: Các đơn vị trực thuộc Bộ

Ngày 10/01/2023, Microsoft đã phát hành danh sách bản vá tháng 01 với 98 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:

- Lỗ hổng bảo mật **CVE-2023-21674** trong Windows Advanced Local Procedure Call (ALPC) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.

- 03 lỗ hổng bảo mật **CVE-2023-21743, CVE-2023-21744, CVE-2023-21742** trong Microsoft SharePoint Server, trong đó **CVE-2023-21743** cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật; 02 lỗ hổng **CVE-2023-21744, CVE-2023-21742** cho phép đối tượng tấn công thực thi mã từ xa.

- 04 lỗ hổng bảo mật **CVE-2023-21763, CVE-2023-21764, CVE-2023-21762, CVE-2023-21745** trong Microsoft Exchange Server, trong đó 02 lỗ hổng **CVE-2023-21763, CVE-2023-21764** cho phép đối tượng tấn công thực hiện nâng cao đặc quyền; 02 lỗ hổng **CVE-2023-21762, CVE-2023-21745** cho phép đối tượng tấn công thực hiện tấn công giả mạo.

- Lỗ hổng bảo mật **CVE-2023-21549** trong Windows Workstation Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã được công bố rộng rãi trên Internet.

- 02 lỗ hổng bảo mật **CVE-2023-21561, CVE-2023-21551** trong Microsoft Cryptographic Services cho phép đối tượng tấn công nâng cao đặc quyền.

- 02 lỗ hổng bảo mật **CVE-2023-21734, CVE-2023-21735** trong Microsoft Office 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 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);
- Cổng thông tin điện tử Bộ KH&CN;
- Lưu: VT, KTHT.

GIÁM ĐỐC

BỘ KHOA HỌC CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM CỦA MICROSOFT
(Kèm theo Công văn số 21 /TTCNTT-KTHT ngày 13 /01 /2023 của Trung tâm Công nghệ thông tin)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-21674	- Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong Windows Advanced Local Procedure Call (ALPC) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21674
2	CVE-2023-21743, CVE-2023-21744, CVE-2023-21742	- Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass), thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21743 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21744 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21742
3	CVE-2023-21763, CVE-2023-21764, CVE-2023-21762, CVE-2023-21745	- Điểm: CVSS: 8.0/7.8 (cao) - Mô tả: lỗ hổng trong trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền, tấn công giả mạo (Spoofing). - Ảnh hưởng: Microsoft Exchange Server 2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21763 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21764 https://msrc.microsoft.com/update-guide/vulnerability/CV

			E-2023-21762 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21745
4	CVE-2023-21549	- Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong Windows Workstation Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã được công bố rộng rãi trên Internet. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2012/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21549
5	CVE-2023-21561, CVE-2023-21551	- Điểm: CVSS: 8.8/7.8 (cao) - Mô tả: lỗ hổng trong Microsoft Cryptographic Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/ 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21561 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21551
6	CVE-2023-21734, CVE-2023-21735	- 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 LTSC for Mac 2021, Microsoft 365, Microsoft Office 2019 for Mac.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21734 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21735

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng bảo mật 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/2023/1/10/the-january-2023-security-update-review

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số 21 /TTCNTT-KTHT ngày 13 /01 /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 Kế hoạch -Tài chính
6	Vụ Pháp chế
7	Vụ Tổ chức cán bộ
8	Vụ Hợp tác quốc tế
9	Vụ Thi đua - Khen thưởng
10	Vụ Phát triển khoa học và công nghệ địa phương
11	Văn phòng Bộ
12	Thanh tra Bộ
13	Cục Công tác phía Nam
14	Cục Ứng dụng và phát triển công nghệ
15	Cục Năng lượng nguyên tử
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	Tổng cục Tiêu chuẩn Đo lường Chất lượng
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