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

Số: 91 /TTCNTT-KTHT

V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 03/2023

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

Hà Nội, ngày 21tháng 03 năm 2023

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

Ngày 14/03/2023, Microsoft đã phát hành danh sách bản vá tháng 03 với 74 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:

a) Sản phẩm của Microsoft cài đặt trên hệ thống thông tin

- Lỗ hổng bảo mật **CVE-2023-23400** trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-24880** 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.

- Lỗ hổng bảo mật **CVE-2023-23392** trong HTTP Protocol Stack cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-23415** trong Internet Control Message Protocol (ICMP) cho phép đối tượng tấn công thực thi mã từ xa.

b) Sản phẩm của Microsoft cài đặt trên máy tính người dùng

- Lỗ hổng bảo mật **CVE-2023-23397** trong Microsoft Outlook 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-2023-24880** 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.

- Lỗ hổng bảo mật **CVE-2023-23392** trong HTTP Protocol Stack cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-23415** trong Internet Control Message Protocol (ICMP) cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-23399** trong trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

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 Kỹ thuật hạ tầng, 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);
- 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 BẢO MẬT TRONG SẢN PHẨM MICROSOFT
(Kèm theo Công văn số 91 /TTCNTT-KTHT ngày 21 / 03 /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-2023-23397	- Điểm: CVSS: 9.1 (nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Outlook, Microsoft Office.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397
2	CVE-2023-24880	- Điểm: CVSS: 5.4 (trung bình) - Mô tả: lỗ hổng 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. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880
3	CVE-2023-23392	- Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hổng trong HTTP Protocol Stack cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server, Windows 11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23392
4	CVE-2023-23415	- Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hổng trong Internet Control Message Protocol (ICMP) 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-2023-23415
5	CVE-2023-23399	- Điểm: CVSS: 7.8 (cao)	https://msrc.microsoft.com/update-

		- Mô tả: lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft Excel, Microsoft 365 .	guide/vulnerability/CVE-2023-23399
6	CVE-2023-23400	- Điểm: CVSS: 7.2 (cao) - Mô tả: lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23400

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/2023/3/14/the-march-2023-security-update-review

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số 91 /TTCNTT-KTHT ngày 21 tháng 03 năm 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