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: 392 /TTCNTT-KTHT
V/v Lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 11/2022

Hà Nội, ngày 15 tháng 11 năm 2022

Kính gửi: Các đơn vị trực thuộc Bộ

Ngày 08/11/2022, Microsoft đã phát hành danh sách bản vá tháng 11 với 64 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:

- 06 lỗ hổng bảo mật **CVE-2022-41082, CVE-2022-41040, CVE-2022-41080, CVE-2022-41079, CVE-2022-41078, CVE-2022-41123** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa, nâng cao đặc quyền. Trong đó, 02 lỗ hổng **CVE-2022-41082**, **CVE-2022-41040** đã được cảnh báo tại Công văn số 339/TTCNTT-KTHT về việc cảnh báo lỗ hổng bảo mật zero-day ảnh hưởng nghiêm trọng đến Microsoft Exchange phát hành ngày 04/10/2022.

- 02 lỗ hổng bảo mật **CVE-2022-41128, CVE-2022-41118** trong Windows Scripting Languages cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật **CVE-2022-41091** trong Windows Mark of the Web cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật.

- Lỗ hổng bảo mật **CVE-2022-41073** trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-41125** trong Windows CNG Key Insolation Service cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- 03 lỗ hổng bảo mật **CVE-2022-41044, CVE-2022-41088, CVE-2022-41039** trong Windows Point-to-Point cho phép đối tượng tấn công thực thi mã từ xa.

- 04 lỗ hổng bảo mật **CVE-2022-41105, CVE-2022-41106, CVE-2022-41063, CVE-2022-41104** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa, tấn công giả mạo (Spoofing), thực hiện tấn công vượt qua cơ chế bảo mật.

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

Nhằm bảo đảm 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, 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

TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

Phụ lục
Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft
(Kèm theo Công văn số 392 /TTCNTT-KTHT ngày 15 /11 /2022 của Trung tâm Công nghệ thông tin)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-41082, CVE-2022-41040, CVE-2022-41080, CVE-2022-41079, CVE-2022-41078, CVE-2022-41123	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa, nâng cao đặc quyền. - Ảnh hưởng: Microsoft Exchange Server 2016 CU 23/22, Exchange Server 2019 CU 11, Exchange Server 2013 CU 23	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41080 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41123 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41078 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41079
2	CVE-2022-41128, CVE-2022-41118	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Windows Scripting Languages cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41128 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41118
3	CVE-2022-41091	- Điểm CVSS: 5.4 (Trung	https://msrc.microsoft.

		bình) - Lỗ hổng trong Windows Mark of the Web cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật. - Ảnh hưởng: Windows 10/11, Windows Server 2016/2019/2022.	com/update-guide/vulnerability/CVE-2022-41091
4	CVE-2022-41073	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41073
5	CVE-2022-41125	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng Windows CNG Key Insolation Service cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019/2022	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41125
6	CVE-2022-41044, CVE-2022-41088, CVE-2022-41039	- Điểm CVSS: 8.1 (Cao) - Lỗ hổng trong Windows Point-to-Point cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41044 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41088 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41039

7	CVE-2022-41105, CVE-2022-41106, CVE-2022-41063, CVE-2022-41104	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa, tấn công giả mạo (Spoofing), thực hiện tấn công vượt qua cơ chế bảo mật. - Ảnh hưởng: Microsoft Excel 2013/2016, Microsoft Office, Microsoft 365.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41105 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41106 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41063 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41104

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. Nguồn tham khảo

https://msrc.microsoft.com/update-guide/releaseNote/2022-Nov
https://www.zerodayinitiative.com/blog/2022/11/8/the-november-2022-security-update-review

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số 392/TTCNTT-KTHT ngày 15/11/2022 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 Hoà 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