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: 35 /TTCNTT-KTHT
V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2022

Hà Nội, ngày 15 tháng 02 năm 2022

Kính gửi: Các đơn vị trực thuộc Bộ

Ngày 08/02/2022, Microsoft đã phát hành danh sách bản vá tháng 02 với 48 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 sau:

- Lỗ hổng bảo mật **CVE-2022-22005** trong Sharepoint Server 2013-2019 cho phép đối tượng tấn công thực thi mã từ xa với tài khoản xác thực hợp lệ.

- Lỗ hổng bảo mật **CVE-2022-21989** trong Windows Kernel cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-21984** trong DNS Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-21995** trong Windows Hyper-V cho phép đối tượng tấn công đã xác thực trên máy khách Hyper-V có thể thực thi mã từ xa trên máy chủ Hyper-V.

- 02 lỗ hổng bảo mật **CVE-2022-22718, CVE-2022-21999** trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- 02 lỗ hổng bảo mật **CVE-2022-22000, CVE-2022-21981** trong Windows Common Log File System Driver cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-21996** trong Windows32k cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-22715** trong Named Pipe File System cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

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 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

BỘ KHOA HỌC VÀ CÔNG NGHỆ
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 35 /TTCNTT-KTHT ngày 15 /02 /2022 của Trung tâm Công nghệ thông tin)

1. Thông tin các lỗ hổng bảo mật

TT	CVE	Mô tả	Link tham khảo
1	CVE-2022-22005	- Điểm CVSS: 8.8 (cao) - Lỗ hổng trong Microsoft SharePoint Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2019, SharePoint Enterprise Server 2013/2016.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22005
2	CVE-2022-21989	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Microsoft Kernel, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2022/2019/2016/2012/2008, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21989
3	CVE-2022-21984	- Điểm CVSS: 8.8 (cao) - Lỗ hổng trong Windows DNS Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10/11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21984
4	CVE-2022-21995	- Điểm CVSS: 7.9 (cao) - Lỗ hổng trong Windows Hyper-V, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10/11, Windows Server 2022/2019/2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21995
5	CVE-2022-22718	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Print Sooler, cho phép đối	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22718

		tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2022/2016/2012/2008, Windows 11/10/8.1/7.	
6	CVE-2022-22000	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Common Log File System Driver, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows Server 2022/2019/2016/2012/2008, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22000
7	CVE-2022-21999	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Print Sooler, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows Server 2022/2016/2012/2008, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21999
8	CVE-2022-21981	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Common Log File System Driver, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows Server 2019/2012/2008, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21981
9	CVE-2022-21996	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows32k, cho phép	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21996

		đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows 11.	
10	CVE-2022-22715	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Named Pipe File System, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows 11/10, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22715

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://www.zerodayinitiative.com/blog/2022/2/8/the-february-2022-security-update-review
https://msrc.microsoft.com/update-guide

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số 35 /TTCNTT-KTHT ngày 15 /02 /2022 của Trung tâm Công nghệ thông tin)

TT	Tên đơn vị
1.	Thanh tra Bộ
2.	Cục Công tác phía Nam
3.	Cục Ứng dụng và phát triển công nghệ
4.	Cục Năng lượng nguyên tử
5.	Cục Thông tin Khoa học và Công nghệ Quốc gia
6.	Cục Phát triển thị trường và doanh nghiệp khoa học và công nghệ
7.	Cục An toàn bức xạ và hạt nhân
8.	Cục Sở hữu trí tuệ
9.	Tổng Cục tiêu chuẩn đo lường chất lượng
10.	Ban quản lý khu công nghệ cao Hoà Lạc
11.	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
12.	Viện Khoa học và công nghệ Việt Nam - Hàn Quốc (VKIST)
13.	Viện Nghiên cứu sáng chế và Khai thác công nghệ
14.	Viện Năng lượng nguyên tử Việt Nam
15.	Viện Ứng dụng công nghệ
16.	Viện Đánh giá khoa học và Định giá công nghệ
17.	Viện Khoa học sở hữu trí tuệ
18.	Viện Nghiên cứu và Phát triển Vùng
19.	Văn phòng các Chương trình trọng điểm cấp nhà nước
20.	Văn phòng Công nhận chất lượng
21.	Văn phòng Đăng ký hoạt động khoa học và công nghệ
22.	Văn phòng các Chương trình khoa học và công nghệ quốc gia
23.	Báo Khoa học và Phát triển
24.	Tạp chí Khoa học và Công nghệ Việt Nam
25.	Nhà xuất bản Khoa học và Kỹ thuật
26.	Quỹ Phát triển khoa học và công nghệ quốc gia
27.	Quỹ Đổi mới công nghệ quốc gia
28.	Trung tâm Nghiên cứu và Phát triển truyền thông khoa học và công nghệ
29.	Trung tâm Nghiên cứu và Phát triển hội nhập khoa học và công nghệ quốc tế