VIỆN HÀN LÂM
KHOA HỌC VÀ CÔNG NGHỆ VN
TRUNG TÂM TIN HỌC VÀ TÍNH TOÁN

Số: 105 /THTT
V/v lỗ hổng bảo mật có mức ảnh hưởng Cao trong các sản phẩm Microsoft công bố tháng 03/2022

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

Hà Nội, ngày21 tháng 3 năm 2022

Kính gửi: Các đơn vị trực thuộc
Viện Hàn lâm Khoa học và Công nghệ Việt Nam

Ngày 08/03/2022, Microsoft đã phát hành danh sách bản vá tháng 03 với 71 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 như sau:

- 02 lỗ hổng bảo mật **CVE-2022 -21990, CVE-2022-23285** trong Remote Desktop Client cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đã có mã khai thác được công bố rộng rãi trên Internet.

- Lỗ hổng bảo mật **CVE-2022 -24459** trong Windows Fax và Scan Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-23277** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa với tài khoản xác thực hợp lệ.

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 các đơn vị, góp phần bảo đảm an toàn cho hệ thống thông tin của Viện Hàn lâm, Trung tâm Tin học và Tính toán khuyến nghị các đơn vị 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.

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.

3. Trong trường hợp cần hỗ trợ, đề nghị liên hệ với Phòng Đảm bảo công nghệ thông tin - Trung tâm Tin học và Tính toán (điện thoại: 024.3791.4773, thư điện tử: *sinhtv@cic.vast.vn*).

Trân trọng./.

Nơi nhận:
- Như trên;
- Viện Hàn lâm KHCNVN (để b/c);
- PCT. Trần Tuấn Anh (để b/c);
- Lưu: VT.

GIÁM ĐỐC

VIỆN HÀN LÂM KHOA HỌC VÀ CÔNG NGHỆ VIỆT NAM
TRUNG TÂM TIN HỌC VÀ TÍNH TOÁN

Phạm Thanh Mai

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT
VÀ HƯỚNG DẪN KHẮC PHỤC
(Kèm theo Công văn số /THTT ngày /3/2022
của Trung tâm Tin học và Tính toán)

1. Thông tin về lỗ hổng bảo mật

STT	Mã lỗ hổng bảo mật	Mô tả
1	CVE-2022-21990	- Lỗ hổng trong Remote Desktop Client cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7 - Điểm CVSS: 8.8 (Cao)
2	CVE-2022-23285	- Lỗ hổng trong Remote Desktop Client cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7 - Điểm CVSS: 8.8 (Cao)
3	CVE-2022-24459	- Lỗ hổng Windows Fax và Scan Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7 - Điểm: CVSS: 7.8 (Cao)
4	CVE-2022-23277	- Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa với tài khoản xác thực hợp lệ. - Ảnh hưởng: Microsoft Exchange Server 2019/2016/2013. - Điểm CVSS: 8.8 (Cao)

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. Các 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-Mar
https://msrc.microsoft.com/update-guide/en-us