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

Số: 327 /THTT
V/v lỗ hổng bảo mật ảnh hưởng Cao trongcác sản phẩm Microsoft công bố tháng 07/2022

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

Hà Nội, ngày27 tháng 7 năm 2022

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

Trung tâm Tin học và Tính toán đã nhận được công văn số 1071/CATTT-NCSC ngày 15 tháng 7 năm 2022 về việc lỗ hổng bảo mật Cao trong các sản phẩm Microsoft công bố tháng 7/2022;

Theo văn bản trên, ngày 12/07/2022, Microsoft đã phát hành danh sách bản vá tháng 07 với 84 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:

- Lỗ hổng bảo mật CVE-2022-22047 trong Windows Client Server Run-Time Subsystem cho phép đối tượng tấn công thực hiện leo thang đặc quyền.

- Lỗ hổng bảo mật CVE-2022-30216 trong Windows Server Service cho phép đối tượng tấn công cài chứng chỉ giả mạo độc hại lên máy chủ mục tiêu từ đó có thể thực hiện các dạng tấn công khác bao gồm tấn công chiếm quyền điều khiển.

- Lỗ hổng bảo mật CVE-2022-22038 trong Remote Procedure Call Runtime cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa.

- 02 Lỗ hổng bảo mật CVE-2022-22029, CVE-2022-22039 trong Windows Network File System cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa.

- 04 lỗ hổng bảo mật CVE-2022-22022, CVE-2022-22041, CVE-2022-30206, CVE-2022-30226 trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. Khai thác thành công, CVE-2022-22041 và CVE-2022-3026 cho phép đối tượng tấn công chiếm quyền điều khiển hệ thống; CVE-2022-22022 và CVE-2022-30226 chỉ cho phép đối tượng tấn công xóa tệp tùy ý trên hệ thống mục tiêu.

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 Khoa học và Công nghệ Việt Nam, 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 thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ais@mic.gov.vn hoặc Trung tâm Tin học và Tính toán: Phòng Đảm bảo Công nghệ thông tin, 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);
- Giám đốc (để b/c);
- Lưu: VT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

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

Phạm Hồng Công

Phụ lục

THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM MICROSOFT

(Kèm theo Công văn số /THTT ngày /7/2022 của Trung tâm Tin học và Tính toán)

1. Thông tin về lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-22047	- Lỗ hổng trong Windows Client Server Run-Time Subsystem cho phép đối tượng tấn công thực hiện leo thang đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11. Windows Server 2008/2012. - Điểm CVSS: 7.8 (Cao)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22047
2	CVE-2022-30216	- Lỗ hổng trong Windows Server Service cho phép đối tượng tấn công cài chứng chỉ giả mạo độc hại lên máy chủ mục tiêu từ đó có thể thực hiện các dạng tấn công khác bao gồm tấn công chiếm quyền điều khiển. - Ảnh hưởng: Windows 10/11, Windows Server. - Điểm CVSS: 8.8 (Cao)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30216
3	CVE-2022-22029	- Lỗ hổng trong trong Windows Network File System cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022. - Điểm CVSS: 8.1 (Cao)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22029
4	CVE-2022-22039	- Lỗ hổng trong trong Windows Network File System cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022. - Điểm CVSS: 7.5 (Cao)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22039
5	CVE-2022-22038	- Lỗ hổng trong trong Remote Procedure Call Runtime cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22038

		012/2016/2019. - Điểm CVSS: 8.1 (Cao)	
6	CVE-2022-30206	- Lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 7/8.1/10, Windows Server 2008/2012/2019/2022 Điểm CVSS: 7.8 (Cao)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30206
7	CVE-2022-22022	- Lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2016/2019/2022 Điểm CVSS: 7.1 (Cao)	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22022
8	CVE-2022-30226	- Lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2019/2022 - Điểm: CVSS: 7.1 (Cao)	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30226
9	CVE-2022-22041	- Lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 8.1/10, Windows Server 2012/2016/2019/2022. - Điểm CVSS: 6.8 (Cao)	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22041

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. Tài liệu tham khảo

https://msrc.microsoft.com/update-guide/releaseNote/2022-Jul

https://www.zerodayinitiative.com/blog/2022/7/12/the-july-2022-security-update-review