BỘ THÔNG TIN TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

Số: 1071 /CATTT-NCSC
V/v lỗ hổng bảo mật ảnh hưởng Cao trong các sản phẩm Microsoft công bố tháng 7/2022

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

Hà Nội, ngày 15 tháng 07năm 2022

Kính gửi:

- Đơn vị chuyên trách về CNTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; các Ngân hàng TMCP; các tổ chức tài chính;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

Ngày 12/7/2022, Microsoft đã phát hành danh sách bản vá tháng 7 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 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 Quý đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Cục An toàn thông tin khuyến nghị Quý 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 (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.

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.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng (để b/c);
- Cục A05, Bộ Công an;
- Bộ Tư lệnh 86, Bộ Quốc phòng;
- Ban Cơ yếu Chính phủ;
- Cục trưởng;
- Trung tâm VNCERT/CC, phòng ATHTTT;
- Lưu: VT, NCSC.

CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Thành Phúc

Phụ lục

Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft

(Kèm theo Công văn số /CATTT-NCSC ngày / /2022 của Cục An toàn thông tin)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-22047	- Điểm CVSS: 7.8 (Cao) - 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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22047
2	CVE-2022-30216	- Điểm CVSS: 8.8 (Cao) - 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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30216
3	CVE-2022-22029	- Điểm CVSS: 8.1 (Cao) - 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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22029
4	CVE-2022-22039	- Điểm CVSS: 7.5 (Cao) - Lỗ hổng trong trong Windows Network File System cho phép đối tượng tấn công không cần	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22039

		xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022.	
5	CVE-2022-22038	- Điểm CVSS: 8.1 (Cao) - 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 2012/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22038
6	CVE-2022-30206	- Điểm CVSS: 7.8 (Cao) - 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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30206
7	CVE-2022-22022	- Điểm CVSS: 7.1 (Cao) - 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.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22022
8	CVE-2022-30226	- Điểm CVSS: 7.1 (Cao) - Lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/12, Windows Server 2008/2012/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30226

9	CVE-2022-22041	- Điểm CVSS: 6.8 (Cao) - 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.	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. 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. 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