UỶ BAN NHÂN DÂN **THÀNH PHỐ BẮC NINH**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1570 /UBND- VHTT V/v cảnh báo, phát hiện, xử lý đảm bảo an toàn thông tin, lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 7/2022	*Thành phố Bắc Ninh, ngày 20 tháng 7 năm 2022*

Kính gửi:
- Các cơ quan, đơn vị thuộc UBND thành phố;
- UBND các phường trên địa bàn thành phố.

Thực hiện Công văn số 520/STTTT- CNTT ngày 18/7/2022 của Sở Thông tin và Truyền thông tỉnh Bắc Ninh về việc lỗ hổng bảo mật ảnh hưởng Cao trong các sản phẩm Microsoft công bố tháng 7/2022;

Tại công văn số 1071/CATTT-NCSC ngày 15/7/2022 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông đã thông báo phát hành danh sách bản vá tháng 7 với 84 lỗ hổng bảo mật có mức ảnh hưởng cao trong các sản phẩm của Microsoft, cụ thể 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.

(Có Phụ lục thông tin chi tiết về các lỗ hổng bảo mật gửi kèm)

Để đảm bảo kịp thời xử lý, khắc phục các lỗ hổng bảo mật về an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị và UBND các phường trên địa bàn thành phố Bắc Ninh (nếu có).

UBND thành phố yêu cầu các cơ quan, đơn vị và UBND các phường triển khai thực hiện tốt một số nhiệm vụ sau:

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.

(Thực hiện theo 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 về an toàn thông tin nhằm phát hiện và xử lý kịp thời các nguy cơ tấn công mạng.

3. Ngay khi phát hiện sự cố, nếu các cơ quan đơn vị và UBND các phường không có khả năng xử lý yêu cầu thông báo về đầu mối Trung tâm Công nghệ Thông tin và Truyền thông - Sở Thông tin và Truyền thông tỉnh Bắc Ninh để được hỗ trợ xử lý, khắc phục kịp thời.

- Đồng chí: Lại Hữu Dương - Phó Giám đốc Trung tâm CNTT&TT, số điện thoại 0913.629.199.

- Đồng chí: Nguyễn Thế Thủy - Phòng Quản trị và Tích hợp hệ thống - Trung tâm CNTT&TT, số điện thoại 0222.3875606 hoặc 0929003888.

- Địa chỉ thư điện tử pqtthht.stttt@bacninh.gov.vn.

Yêu cầu các cơ quan, đơn vị và UBND các phường nghiêm túc triển khai thực hiện./.

Nơi nhận:
- Như kính gửi (t/h);
- TT Thành ủy - HĐND thành phố (b/c);
- Chủ tịch, các PCT UBND thành phố;
- Lưu: VT, VHTT.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Mạnh Hiếu

PHỤ LỤC
Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft
(Kèm theo Công văn số 1570 /UBND-VHTT ngày 20 /7/2022 của UBND thành phố Bắc Ninh)

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/updateguide/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/updateguide/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/updateguide/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 xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/updateguide/enUS/vulnerability/CVE2022-22039

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/updateguide/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/updateguide/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/updateguide/enUS/vulnerability/CVE2022- 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/updateguide/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/updateguide/enUS/vulnerability/CVE2022-22041

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 cơ quan, đơn vị tham khảo 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