BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 2604/BTTTT - CATTT V/v 05 lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft	*Hà Nội, ngày 16 tháng 7 năm 2021*

Kính gửi:

- Các Bộ, Cơ quan ngang Bộ, Cơ quan thuộc Chính phủ;
- Văn phòng Trung ương Đảng, Văn phòng Chủ tịch nước, Văn phòng Quốc hội, Tòa án nhân dân tối cao, Viện Kiểm sát nhân dân tối cao, Kiểm toán Nhà nước;
- UBND các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn kinh tế, Tổng công ty Nhà nước, các Ngân hàng TMCP; các tổ chức tài chính.

Ngày 13/7/2021, Microsoft đã công bố và phát hành bản vá cho 117 lỗ hổng bảo mật trong các sản phẩm của mình, trong đó đáng chú ý là **05** lỗ hổng bảo mật (CVE-2021-34473, CVE-2021-34523, CVE-2021-34527, CVE-2021-33781, CVE-2021-34492) trong các sản phẩm Windows Print Spooler, Microsoft Exchange Server và Windows Certificate, cho phép đối tượng tấn công thực thi mã từ xa. Các sản phẩm này của Microsoft đều được sử dụng phổ biến trong các hệ thống thông tin cơ quan, tổ chức nhà nước; ngân hàng, tổ chức tài chính, tập đoàn, doanh nghiệp và các công ty lớn. Đặc biệt các lỗ hổng bảo mật trong **Windows Print Spooler** và **Microsoft Exchange Server** có thể đã, đang và sẽ được các nhóm tấn công có chủ đích (APT) sử dụng để khai thác diện rộng trong thời gian sắp tới. Thông tin cụ thể về các lỗ hổng như sau:

- 02 lỗ hổng CVE-2021-34473, CVE-2021-34523: tồn tại trong Microsoft Exchange Server, cho phép đối tượng tấn công có thể thực thi mã từ xa, nâng cao đặc quyền trên máy chủ thư điện tử. Exchange Server đã trở thành một mục tiêu khá phổ biến kể từ tháng 3/2021 nổi bật với 04 lỗ hổng Zero-days hay còn gọi là ProxyLogon đã được khai thác trong chiến dịch tấn công APT trên diện rộng. 04 lỗ hổng này cũng đã được Trung tâm Giám sát an toàn không gian mạng quốc gia

(NCSC), Cục An toàn thông tin, Bộ Thông tin và Truyền thông cảnh báo tại công văn số 13/NCSC-ĐTPT về việc lỗ hổng bảo mật trong Microsoft Exchange Server ngày 03/3/2021. Vì vậy, khắc phục các lỗ hổng trong Exchange Server là hết sức cấp thiết khi việc đối tượng tấn công mạng đang ngày càng gia tăng nhằm mục tiêu này.

- Lỗ hổng CVE-2021-34527: thực thi mã từ xa thứ 2 trong Windows Print Spooler (liên quan đến lỗ hổng CVE-2021-1675 trước đó). 02 lỗ hổng này đang được gọi với cái tên là "PrinterNightmare". Bộ Thông tin và Truyền thông đã có dự báo sớm cho các lỗ hổng này tại công văn số 2210/BTTTT-CATTT về việc dự báo sớm nguy cơ tấn công mạng trên diện rộng ngày 22/6/2021, đồng thời cũng đã kịp thời tiếp tục cảnh báo đến các cơ quan, tổ chức thông qua nhiều phương thức tiếp cận khác nhau.

- Lỗ hổng CVE-2021-33781: lỗ hổng cho phép đối tượng có đặc quyền thấp tấn công từ xa vượt qua các cơ chế kiểm tra bảo mật trong dịch vụ Active Directory để đạt được các đặc quyền cao hơn trên máy mục tiêu.

- Lỗ hổng CVE-2021-34492: lỗ hổng cho phép đối tượng tấn công vượt qua cơ chế kiểm tra trong Windows Certificate để giả mạo chứng chỉ. Lỗ hổng này là hoàn toàn có thể được dùng trong các cuộc tấn công khác nhằm vào người dùng.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý cơ quan, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Bộ Thông tin và Truyền thông yêu cầu Quý cơ quan chỉ đạo thực hiện:

1. Kiểm tra, rà soát và xác định máy chủ, máy trạm sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá bảo mật cho các máy bị ảnh hưởng theo hướng dẫn của Microsoft (chi tiết tham khảo 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 hỗ trợ, Quý đơn vị liên hệ đầu mối hỗ trợ của Bộ Thông tin và Truyền thông: Trung tâm Giám sát an toàn không gian mạng quốc

gia (NCSC), Cục An toàn thông tin, điện thoại: 02432091616, thư điện tử: ais@mic.gov.vn

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ Công an;
- Bộ Quốc phòng;
- Ban Cơ yếu Chính phủ;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng;
- Lưu: VT, Cục ATTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nguyễn Huy Dũng

Phụ lục

Thông tin lỗ hổng bảo mật

(Kèm theo Công văn số 2609/BTTTT-CATTT ngày 16 / 7 /2021 của Bộ Thông tin và Truyền thông)

1. Thông tin lỗ hổng bảo mật

TT	CVE	Mô tả	Ghi chú
1	CVE-2021-34473	- **Mô tả:** Lỗ hổng tồn tại trong Microsoft Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa. - **Điểm CVSS:** 9.1 (cao) - **Ảnh hưởng:** Exchange Server 2019/2016/2013 - **Nguồn tham khảo:** https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473	- Công văn số 13/NCSC-ĐTPT về việc lỗ hổng bảo mật trong Microsoft Exchange Server ngày 03/3/2021. - Công văn số 1122/BTTTT-CATTT về việc 04 lỗ hổng bảo mật mới ảnh hưởng nghiêm trọng tới máy chủ thư điện tử Microsoft Exchange Server và hướng dẫn xử lý ngày 16/4/2021.
2	CVE-2021-34523	- **Mô tả:** Lỗ hổng tồn tại trong Microsoft Exchange Server, cho phép đối tượng tấn công thực thi mã từ xa. - **Điểm CVSS:** 9.1 (cao) - **Ảnh hưởng:** Exchange Server 2019/2016/2013 - **Nguồn tham khảo:** https://msrc.microsoft.com/update-	Lỗ hổng mới công bố ngày 13/7/2021.

		guide/vulnerability/CVE-2021-34523	
3	CVE-2021-34527	**- Mô tả:** Lỗ hổng tồn tại trong Windows Print Spooler, cho phép đối tượng tấn công thực thi mã từ xa. **- Điểm CVSS:** 8.8 (cao) **- Nguồn tham khảo:** https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527	- Công văn số 2210/BTTTT-CATTT về việc dự báo sớm nguy cơ tấn công mạng trên diện rộng ngày 22/6/2021. - Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin, Bộ Thông tin và truyền thông đã có cảnh báo rộng rãi gửi trực tiếp đến các cơ quan tổ chức thông qua thư điện tử, Page FB chính thức của NCSC.
4	CVE-2021-33781	**- Mô tả:** Lỗ hổng cho phép đối tượng có đặc quyền thấp tấn công từ xa vượt qua các cơ chế kiểm tra bảo mật trong dịch vụ Active Directory để đạt được các đặc quyền cao hơn trên máy mục tiêu. **- Điểm CVSS:** 8.1 (cao) **- Ảnh hưởng:** Windows 10, Windows Server 2019. **- Nguồn tham khảo:** https://msrc.microsoft.com/update-	Lỗ hổng mới công bố ngày 13/7/2021.

		guide/vulnerability/CVE-2021-33781	
5	CVE-2021-34492	- **Mô tả:** Lỗ hổng cho phép đối tượng tấn công vượt qua cơ chế kiểm tra trong Windows Certificate để giả mạo chứng chỉ. - **Điểm CVSS:** 8.1 (cao) - **Ảnh hưởng:** Windows 10/8.1/RT8.1/7, Windows Server 2016/2012/2008. - **Nguồn tham khảo:** https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34492	Lỗ hổng mới công bố ngày 13/7/2021.

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục lỗ hổng bảo mật này là cập nhật bản vá. Trong trường hợp chưa thể cập nhật bản vá kịp thời, Quý đơn vị thực hiện các biện pháp khắc phục theo hướng dẫn của hãng, để giảm thiểu nguy cơ tấn công (tham khảo tại nguồn link được thống kê ở bảng trên)

3. Nguồn tham khảo

- Bản vá tháng 7 của Microsoft:

https://msrc.microsoft.com/update-guide

https://msrc.microsoft.com/update-guide/releaseNote/2021-Jul

- Đánh giá của Zero Day Initiative:

https://zerodayinitiative.com/blog/2021/7/13/the-july-2021-security-update-review