BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

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

Số: 203 /TTCNTT-KTHT
V/v các lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft

Hà Nội, ngày 22 tháng 07năm 2021

Kính gửi: Các đơn vị trực thuộc Bộ

Theo Công văn số 2604/BTTTT-CATTT ngày 16/7/2021 của Bộ Thông tin và Truyền thông về việc 05 lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft, 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 của 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 đã được Trung tâm Công nghệ thông tin cảnh báo tại Công văn số 61/TTCNTT-KTHT ngày 19/3/2021 về việc lỗ hổng bảo mật trong Microsoft Exchange Server. Vì vậy, khắc phục các lỗ hổng trong Exchange Server là hết sức cấp thiết khi các 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". Trung tâm Công nghệ thông tin đã có dự báo sớm cho các lỗ hổng này tại Công văn số 171/TTCNTT-KTHT ngày 30/6/2021 về việc dự báo sớm nguy cơ tấn công mạng trên diện rộng. Ngày 15/7/2021, sau lỗ hổng "PrinterNightmare" Microsoft lại tiếp tục công bố lỗ hổng bảo mật (CVE-2021-34481) trong Windows Print Spooler có điểm CVSS: 7.8 (cao), cho phép đối tượng tấn công thực thi mã từ xa với đặc quyền cao hơn trong máy mục tiêu. Tuy nhiên lỗ hổng này được cho là không liên quan đến lỗ hổng

"PrinterNightmare" trước đó. Lỗ hổng chỉ có thể khai thác cục bộ để đạt được các đặc quyền nâng cao trên một thiết bị. Tại thời điểm này chưa có bản vá cho lỗ lổng bảo mật này.

- 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 bảo đảm an toàn thông tin cho hệ thống thông tin của Quý đơn vị, Trung tâm Công nghệ thông tin khuyến nghị Quý đơn 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 thiết, Quý đơn vị liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, điện thoại 024.39439060, thư điện tử: phongktht@most.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Cổng thông tin điện tử Bộ KH&CN;
- Lưu: VT, KTHT.

GIÁM ĐỐC

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

Phụ lục
Thông tin lỗ hổng bảo mật
(Kèm theo Công văn số 203/TTCNTT-KTHT ngày 22/07/2021 của Trung tâm Công nghệ thông tin)

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 61/TTCNTT-KTHT ngày 19/3/2021 về việc lỗ hổng bảo mật trong Microsoft Exchange Server. - Công văn số 88/TTCNTT-KTHT ngày 20/4/2021 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.
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-guide/vulnerability/CVE-2021-34523	Lỗ hổng mới công bố ngày 13/7/2021.
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. Ảnh hưởng tới các máy tính cá nhân. - **Điểm** CVSS: 8.8 (cao) - **Nguồn tham khảo:** https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527	Công văn số 171/TTCNTT-KTHT ngày 30/6/2021 về việc dự báo sớm nguy cơ tấn công mạng trên diện rộng.
4	CVE-2021-34481	- **Mô tả:** Lỗ hổng tồn tại trong Windows Print Spooler, cho phép đối tượng tấn công thực thi mã từ xa	Lỗ hổng mới công bố ngày 15/7/2021. Thực hiện biện pháp giảm

		với đặc quyền cao hơn trong máy mục tiêu. **- Điểm** CVSS: 7.8 (cao) **- Nguồn tham khảo:** https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481	thiếu nguy cơ tấn công cho lỗ hổng bảo mật bằng cách tắt dịch vụ Print Spooler
5	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-guide/vulnerability/CVE-2021-33781	Lỗ hổng mới công bố ngày 13/7/2021.
6	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 các 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

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số 203/TTCNTT-KTHT ngày 22/07/2021 của Trung tâm Công nghệ thông tin)

TT	Tên đơn vị
1.	Thanh tra Bộ
2.	Cục Công tác phía Nam
3.	Cục Ứng dụng và phát triển công nghệ
4.	Cục Năng lượng nguyên tử
5.	Cục Thông tin Khoa học và Công nghệ Quốc gia
6.	Cục Phát triển thị trường và doanh nghiệp khoa học và công nghệ
7.	Cục An toàn bức xạ và hạt nhân
8.	Cục Sở hữu trí tuệ
9.	Tổng Cục tiêu chuẩn đo lường chất lượng
10.	Ban quản lý khu công nghệ cao Hoà Lạc
11.	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
12.	Viện Khoa học và công nghệ Việt Nam - Hàn Quốc (VKIST)
13.	Viện Nghiên cứu sáng chế và Khai thác công nghệ
14.	Viện Năng lượng nguyên tử Việt Nam
15.	Viện Ứng dụng công nghệ
16.	Viện Đánh giá khoa học và Định giá công nghệ
17.	Viện Khoa học sở hữu trí tuệ
18.	Viện Nghiên cứu và Phát triển Vùng
19.	Văn phòng các Chương trình trọng điểm cấp nhà nước
20.	Văn phòng Công nhận chất lượng
21.	Văn phòng Đăng ký hoạt động khoa học và công nghệ
22.	Văn phòng các Chương trình khoa học và công nghệ quốc gia
23.	Báo Khoa học và Phát triển
24.	Tạp chí Khoa học và Công nghệ Việt Nam
25.	Nhà xuất bản Khoa học và Kỹ thuật
26.	Quỹ Phát triển khoa học và công nghệ quốc gia
27.	Quỹ Đổi mới công nghệ quốc gia
28.	Trung tâm Nghiên cứu và Phát triển truyền thông khoa học và công nghệ
29.	Trung tâm Nghiên cứu và Phát triển hội nhập khoa học và công nghệ quốc tế