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: 233 /TTCNTT-KTHT
V/v 10 lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft

Hà Nội, ngày 17 tháng 08năm 2021

Kính gửi: Các đơn vị trực thuộc Bộ

Ngày 10/8/2021 vừa qua, Microsoft phát hành danh sách bản vá lỗi tháng 8/2021 với 44 bản vá cho các lỗ hổng bảo mật trong sản phẩm của mình, 13 trong số 44 lỗ hổng được công bố lần này là lỗ hổng bảo mật cho phép thực thi mã từ xa, 7 lỗ hổng trong số này được đánh giá là quan trọng. Trong đó đáng chú ý là 10 lỗ hổng bảo mật có mức ảnh hưởng tương đối lớn trong các sản phẩm Microsoft (thông tin chi tiết có tại Phụ lục kèm theo), đặc biệt là **04** lỗ hổng bảo mật tồn tại trong Windows Print Spooler và Microsoft Windows. Cụ thể như sau:

- **03** lỗ hổng bảo mật **(CVE-2021-36936, CVE-2021-36947, CVE-2021-34483)** trong Windows Print Spooler: cho phép đối tượng tấn công thực thi mã từ xa, nâng cao đặc quyền. Trong 2 tháng vừa qua, lỗ hổng trong Print Spooler đã có ảnh hưởng khá lớn và được quan tâm đặc biệt khi mà Microsoft liên tục công bố bản vá cho các lỗ hổng liên quan, bắt đầu với CVE-2021-1675 vào tháng 6, tiếp theo là bản vá lỗi cho CVE-2021-34527 (còn được gọi là PrintNightmare) vào tháng 7. Công cụ để khai thác các lỗ hổng trên đã được công bố rộng rãi trên Internet nên nguy cơ bị khai thác bởi các nhóm tấn công APT hoặc được sử dụng trong các cuộc tấn công diện rộng là rất lớn. 02 lỗ hổng này đã được cảnh báo tại Công văn số 203/TTCNTT-KTHT ngày 22/7/2021 về việc các lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft và Công văn số 171/TTCNTT-KTHT ngày 30/6/2021 về việc dự báo sớm nguy cơ tấn công mạng trên diện rộng.

- Lỗ hổng bảo mật **(CVE-2021-26424)** trong Microsoft Windows: là lỗ hổng TCP/IP, cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này ảnh hưởng đến Windows 7 đến 10 và Windows Server 2008 đến 2019 với điểm CVSS: 9.9 (Nghiêm trọng). Tuy vậy theo dự đoán của Cục An toàn thông tin – Bộ Thông tin và Truyền thông, mã khai thác của lỗ hổng này sẽ khó được công bố sớm do việc phát triển mã khai thác phải vượt qua các tính năng bảo vệ trong các phiên bản mới của Windows.

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 vị 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

Hà Quốc Trung

Phụ lục
Thông tin các lỗ hổng bảo mật
(Kèm theo Công văn số 233/TTCNTT-KTHT ngày 17 /08/2021 của Trung tâm Công nghệ thông tin)

1. Thông tin các lỗ hổng bảo mật

TT	CVE	Mô tả	Ghi chú
1	CVE-2021-36947	- **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) - **Ảnh hưởng:** Windows 7/8.1/10 và Windows Server 2008/2012/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473
	CVE-2021-36936	- **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) - **Ảnh hưởng:** Windows 7/8.1/10 và Windows Server 2008/2012/2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36936
	CVE-2021-34483	- **Mô tả:** Lỗ hổng tồn tại trong Windows Print Spooler, cho phép đối tượng tấn công nâng cao đặc quyền. - **Điểm CVSS:** 7.8 (Cao) - **Ảnh hưởng:** Windows 7/8.1/10 và Windows Server 2008/2012/2016.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34483
2	CVE-2021-26424	- **Mô tả:** Lỗ hổng tồn tại liên quan đến giao thức TCP/IP của Windows, cho phép đối tượng tấn công thực thi mã từ xa. - **Điểm CVSS:** 9.9 (Nghiêm trọng) - **Ảnh hưởng:** Windows 7 đến 10 và Windows Server 2008 đến 2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26424
3	CVE-2021-34535	- **Mô tả:** Lỗ hổng tồn tại trong Remote Desktop Client, cho phép đối tượng tấn công thực thi mã từ xa. - **Điểm CVSS:** 8.8 (Cao)	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34535

		- **Ảnh hưởng:** Windows 7/8.1/10 và Windows Server 2008/2012/2019.	
4	CVE-2021-36948	- **Mô tả:** Lỗ hổng tồn tại trong Windows Update Medic Service (WaasMedic), cho phép đối tượng tấn công nâng cao đặc quyền. - **Điểm CVSS:** 7.8 (Cao) - **Ảnh hưởng:** Windows 10 và Windows Server 2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36948
5	CVE-2021-36942	- **Mô tả:** Lỗ hổng tồn tại trong Windows Local Security Authority (LSA), cho phép đối tượng tấn công thực hiện tấn công giả mạo. - **Điểm CVSS:** 7.5 (Cao) - **Ảnh hưởng:** Windows 10 và Windows Server 2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36942
6	CVE-2021-36941	- **Mô tả:** Lỗ hổng tồn tại trong Microsoft Word, cho phép đối tượng tấn công thực thi mã từ xa. - **Điểm CVSS:** 7.8 (Cao) - **Ảnh hưởng:** Microsoft 365, Microsoft Office 2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36941
7	CVE-2021-34478	- **Mô tả:** Lỗ hổng tồn tại trong Microsoft Office, cho phép đối tượng tấn công thực thi mã từ xa. - **Điểm CVSS:** 7.8 (Cao) - **Ảnh hưởng:** Microsoft 365, Microsoft Office 2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34478
8	CVE-2021-34524	- **Mô tả:** Lỗ hổng tồn tại trong Microsoft Dynamics 365 (on-premises), cho phép đối tượng tấn công thực thi mã từ xa. - **Điểm CVSS:** 8.1 (Cao) - **Ảnh hưởng:** Microsoft Dynamics 365 (on-premises) version 9.0 và 9.1	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34524
9	CVE-2021-26426	- **Mô tả:** Lỗ hổng tồn tại trong Windows User Profile Service cho phép đối tượng tấn công nâng cao đặc quyền. - **Điểm CVSS:** 7.8 (Cao)	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26426

		- **Ảnh hưởng:** Windows Server 2008/2012/2016/2019, Windows 7/8.1/10	
10	CVE-2021-34484	- **Mô tả:** Lỗ hổng tồn tại trong Windows User Profile Service cho phép đối tượng tấn công nâng cao đặc quyền. - **Điểm CVSS:** 7.8 (Cao) - **Ảnh hưởng:** Windows Server 2008/2012/2016/2019, Windows 7/8.1/10	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34484

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 8 của Microsoft:

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

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

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số 233/TTCNTT-KTHT ngày 17 /08/2021 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 Hòa 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