BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

Số: 603 /CNTT-YTĐT

V/v 10 lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft

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

Hà Nội, ngày 18 tháng 08 năm 2021

Kính gửi:

- Vụ, Cục, Tổng cục, Văn phòng Bộ, Thanh tra Bộ;
- Các đơn vị trực thuộc Bộ Y tế;
- Các Sở Y tế.

Cục Công nghệ thông tin nhận được Công văn số 1115/CATTT-NCSC ngày 13/8/2021 của Cục An toàn thông tin về việc 10 lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin, Cục Công nghệ thông tin trân trọng đề nghị Quý đơn vị:

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 Trung tâm Dữ liệu y tế, Cục Công nghệ thông tin, Bộ Y tế (ThS. Hoàng Đăng Trị, điện thoại: 0987772483; Email: trihd.cntt@moh.gov.vn) để được hỗ trợ.

Trân trọng./.

Nơi nhận:
- Như trên;
- Cục trưởng (để b/c);
- Trung tâm Dữ liệu y tế (để thực hiện);
- Lưu: VT, CNTT.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN
BỘ Y TẾ

Phạm Xuân Viết

BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

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

THÔNG TIN LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số /CNTT-YTĐT ngày /8/2021 của Cục Công nghệ thông tin)

1. Thông tin lỗ hổng bảo mật

TT	CVE	Mô tả	Ghi chú
1	CVE-2021-36947	- 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-2021-36947
	CVE-2021-36936	- 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	- 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	- 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	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26424

		2008 đến 2019.	
3	CVE-2021-34535	- Lỗ hổng tồn tại trong Remote Desktop Client, 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-2021-34535
4	CVE-2021-36948	- 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	- 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	- 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	- 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	- 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)	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34524

		- Ảnh hưởng: Microsoft Dynamics 365 (on-premises) version 9.0 và 9.1	
9	CVE-2021-26426	- 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-2021-26426
10	CVE-2021-34484	- 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 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