

UBND THÀNH PHỐ HÀ NỘI  
**SỞ Y TẾ**

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

Số: ~~13699~~ /SYT-KHTC  
V/v 10 lỗ hồng bảo mật mức cao và  
nghiêm trọng trong các sản phẩm  
Microsoft.

Hà Nội, ngày 01 tháng 9 năm 2021

Kính gửi: Các đơn vị trực thuộc Ngành Y tế Hà Nội.

Thực hiện Công văn số 603/CNTT-YTĐT ngày 18/8/2021 của Cục Công nghệ thông tin, Bộ Y tế và Công văn số 2242/STTTT-CNTT ngày 19/8/2021 của Sở Thông tin và Truyền thông về việc 10 lỗ hồng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft. Để đảm bảo an toàn thông tin đối với các hệ thống thông tin, Sở Y tế đề nghị các đơn vị một số nội dung sau:

1. Nghiên cứu Công văn số 603/CNTT-YTĐT ngày 18/8/2021 của Cục Công nghệ thông tin, Bộ Y tế, Công văn số 2242/STTTT-CNTT ngày 19/8/2021 của Sở Thông tin và Truyền thông và tổ chức triển khai thực hiện theo quy định (văn bản kèm theo).

2. Chủ động rà soát các hệ thống thông tin của đơn vị, sẵn sàng phương án xử lý khi phát hiện có dấu hiệu khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng, các tổ chức lớn về an toàn thông tin để phát hiện kịp thời nguy cơ tấn công mạng và các lỗ hồng bảo mật.


Trong quá trình triển khai thực hiện, nếu có khó khăn vướng mắc đề nghị các đơn vị liên hệ:



- Phòng Công nghệ thông tin, Sở Thông tin và Truyền thông (điện thoại: 024.37366621, email: pcntt\_sotttt@hanoi.gov.vn).

- Đội ứng cứu sự cố an toàn thông tin mạng thành phố Hà Nội của Sở Thông tin và Truyền thông (điện thoại trực 24/7: 024.35124010, email: ttddl\_sotttt@hanoi.gov.vn).

Sở Y tế yêu cầu các đơn vị nghiên cứu triển khai thực hiện theo quy định.

Nơi nhận: 

- Như trên;
- Sở TT&TT (để phối hợp);
- Giám đốc Sở (để báo cáo);
- Lưu: VT, KHTC. 

KT. GIÁM ĐỐC  
PHÓ GIÁM ĐỐC   
  
Trần Văn Chung

**BỘ Y TẾ  
CỤC CÔNG NGHỆ THÔNG TIN**

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

Số: 603 /CNTT-YTĐT

Hà Nội, ngày 18 tháng 08 năm 2021

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

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.

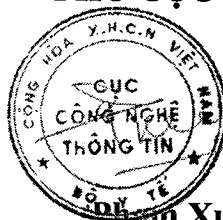
Trong trường hợp cần thiết, Quý Đơn vị liên hệ Trung tâm Dữ liệu y tế, Cục Công nghệ thông tin, Bộ Y tế (ThS. Hoàng Đăng Trị, điện thoại: 0987772483; Email: trihd.cntt@moh.gov.vn) để được hỗ trợ.

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**



**Phạm Xuân Viêt**

**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	<ul style="list-style-type: none"><li>- Lỗ hổng tồn tại trong Windows Print Spooler, cho phép đối tượng tấn công thực thi mã từ xa.</li><li>- Điểm CVSS: 8.8 (Cao)</li><li>- Ảnh hưởng: Windows 7/8.1/10 và Windows Server 2008/2012/2019.</li></ul>	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36947">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36947</a>
	CVE-2021-36936	<ul style="list-style-type: none"><li>- Lỗ hổng tồn tại trong Windows Print Spooler, cho phép đối tượng tấn công thực thi mã từ xa.</li><li>- Điểm CVSS: 8.8 (Cao)</li><li>- Ảnh hưởng: Windows 7/8.1/10 và Windows Server 2008/2012/2019.</li></ul>	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36936">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36936</a>
	CVE-2021-34483	<ul style="list-style-type: none"><li>- Lỗ hổng tồn tại trong Windows Print Spooler, cho phép đối tượng tấn công nâng cao đặc quyền.</li><li>- Điểm CVSS: 7.8 (Cao)</li><li>- Ảnh hưởng: Windows 7/8.1/10 và Windows Server 2008/2012/2016.</li></ul>	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34483">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34483</a>
2	CVE-2021-26424	<ul style="list-style-type: none"><li>- Lỗ hổng tồn tại liên quan đến giao thức TCP/IP của Windows, cho phép đối tượng tấn công thực thi mã từ xa.</li><li>- Điểm CVSS: 9.9 (Nghiêm trọng)</li><li>- Ảnh hưởng: Windows 7 đến 10 và Windows Server</li></ul>	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26424">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26424</a>

		2008 đến 2019.	
3	CVE-2021-34535	<ul style="list-style-type: none"> <li>- Lỗ hổng tồn tại trong Remote Desktop Client, cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Điểm CVSS: 8.8 (Cao)</li> <li>- Ảnh hưởng: Windows 7/8.1/10 và Windows Server 2008/2012/2019.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34535">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34535</a>
4	CVE-2021-36948	<ul style="list-style-type: none"> <li>- Lỗ hổng tồn tại trong Windows Update Medic Service (WaasMedic), cho phép đối tượng tấn công nâng cao đặc quyền.</li> <li>- Điểm CVSS: 7.8 (Cao)</li> <li>- Ảnh hưởng: Windows 10 và Windows Server 2019.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36948">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36948</a>
5	CVE-2021-36942	<ul style="list-style-type: none"> <li>- Lỗ hổng tồn tại trong Windows Local Security Authority (LSA), cho phép đối tượng tấn công thực hiện tấn công giả mạo.</li> <li>- Điểm CVSS: 7.5 (Cao)</li> <li>- Ảnh hưởng: Windows 10 và Windows Server 2019.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36942">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36942</a>
6	CVE-2021-36941	<ul style="list-style-type: none"> <li>- Lỗ hổng tồn tại trong Microsoft Word, cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Điểm CVSS: 7.8 (Cao)</li> <li>- Ảnh hưởng: Microsoft 365, Microsoft Office 2019.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36941">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36941</a>
7	CVE-2021-34478	<ul style="list-style-type: none"> <li>- Lỗ hổng tồn tại trong Microsoft Office, cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Điểm CVSS: 7.8 (Cao)</li> <li>- Ảnh hưởng: Microsoft 365, Microsoft Office 2019.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34478">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34478</a>
8	CVE-2021-34524	<ul style="list-style-type: none"> <li>- Lỗ hổng tồn tại trong Microsoft Dynamics 365 (on-premises), cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Điểm CVSS: 8.1 (Cao)</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34524">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34524</a>

		- 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	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26426">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26426</a>
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	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34484">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34484</a>

## 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>

**UBND THÀNH PHỐ HÀ NỘI**  
**SỞ THÔNG TIN VÀ TRUYỀN THÔNG**

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

Số: 2242/STTTT-CNTT  
V/v cảnh báo 10 lỗ hổng bảo mật mức cao và  
nghiêm trọng trong các sản phẩm Microsoft.

Hà Nội, ngày 19 tháng 8 năm 2021

Kính gửi:

- Các sở, ban, ngành;
- UBND các quận, huyện, thị xã.

Sở Thông tin và Truyền thông nhận được Công văn số 1115/CATTT-NCSC ngày 13/8/2021 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc 10 lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft (*bản chụp kèm theo*), để đảm bảo an toàn, an ninh thông tin cho các hệ thống Sở Thông tin và Truyền thông đề nghị các cơ quan thuộc UBND Thành phố:

1. Khẩn trương kiểm tra, rà soát, xác minh hệ thống thông tin, máy chủ, máy trạm có khả năng bị ảnh hưởng bởi các lỗ hổng trên; tiến hành cập nhật bản vá lỗ hổng bảo mật (nếu có) cho các máy chủ, máy trạm bị ảnh hưởng theo hướng dẫn tại công văn số 1115/CATTT-NCSC.

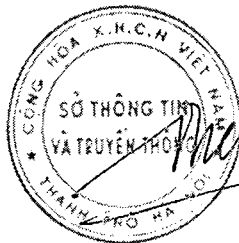
2. Tăng cường giám sát an toàn an ninh thông tin, kịp thời phát hiện hoạt động bị khai thác, tấn công mạng và xử lý các lỗ hổng bảo mật (nếu có).

Trong trường hợp cần hỗ trợ ứng cứu sự cố tấn công mạng, đề nghị các đơn vị liên hệ Phòng Công nghệ Thông tin - Sở Thông tin và Truyền thông (điện thoại: 024.37366621, email: pcntt\_sotttt@hanoi.gov.vn) hoặc Đội ứng cứu sự cố an toàn thông tin mạng thành phố Hà Nội (điện thoại trực 24/7: 0243. 5124010; Email: ttdl\_sotttt@hanoi.gov.vn) để phối hợp xử lý./.

**Nơi nhận :**

- Như trên;
- Giám đốc Sở TT&TT;
- Các Phó Giám đốc Sở TT&TT;
- TTDLNN, Đội UCSC;
- Lưu: VT, CNTT(Người).

**GIÁM ĐỐC**



**Nguyễn Thanh Liêm**