

BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

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

Số: /CNTT-YTĐT
V/v lỗ hổng bảo mật ảnh hưởng cao
và nghiêm trọng trong các sản phẩm
Microsoft công bố tháng 02/2022

Hà Nội, ngày tháng năm 2022

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 163 /CATTT-NCSC ngày 09/02/2022 của Cục An toàn thông tin về lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2022.

Ngày 08/02/2022, Microsoft đã phát hành danh sách bản vá tháng 02 với 48 lỗ hổng bảo mật trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý các lỗ hổng bảo mật có mức ảnh hưởng cao sau:

- Lỗ hổng bảo mật **CVE-2022-22005** trong Sharepoint Server 2013-2019 cho phép đối tượng tấn công thực thi mã từ xa với tài khoản xác thực hợp lệ.

- Lỗ hổng bảo mật **CVE-2022-21989** trong Windows Kernel cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-21984** trong DNS Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-21995** trong Windows Hyper-V cho phép đối tượng tấn công đã xác thực trên máy khách Hyper-V có thể thực thi mã từ xa trên máy chủ Hyper-V.

- 02 lỗ hổng bảo mật **CVE-2022-22718, CVE-2022-21999** trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- 02 lỗ hổng bảo mật **CVE-2022-22000, CVE-2022-21981** trong Windows Common Log File System Driver cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-21996** trong Windows32k cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-22715** trong Named Pipe File System cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

Thông tin chi tiết các lỗ hổng bảo mật có tại phụ lục kèm theo

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

1. Kiểm tra, rà soát, xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công (tham khảo thông tin 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 Tri, điện thoại: 0987772483; Email: trihd.cntt@moh.gov.vn) để được hỗ trợ.

Trân trọng./.

Nơi nhận:

- Như trên;
- Trung tâm Dữ liệu y tế (để thực hiện);
- Lưu: VT, CNTT.

CỤC TRƯỞNG

Đỗ Trường Duy

THÔNG TIN LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số /CNTT-YTĐT ngày / /2022
của Cục Công nghệ thông tin)

1. Thông tin lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-22005	<ul style="list-style-type: none">- Điểm CVSS: 8.8 (cao)- Lỗ hổng trong Microsoft SharePoint Server, cho phép đối tượng tấn công thực thi mã từ xa.- Ảnh hưởng: Microsoft SharePoint Server 2019, SharePoint Enterprise Server 2013/2016.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22005
2	CVE-2022-21989	<ul style="list-style-type: none">- Điểm CVSS: 7.8 (cao)- Lỗ hổng trong Microsoft Kernel, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.- Ảnh hưởng: Windows Server 2022/2019/2016/2012/2008, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21989
3	CVE-2022-21984	<ul style="list-style-type: none">- Điểm CVSS: 8.8 (cao)- Lỗ hổng trong Windows DNS Server, cho phép đối tượng tấn công thực thi mã từ xa.- Ảnh hưởng: Windows 10/11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21984

4	CVE-2022-21995	<ul style="list-style-type: none"> - Điểm CVSS: 7.9 (cao) - Lỗ hổng trong Windows Hyper-V, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10/11, Windows Server 2022/2019/2016. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21995
5	CVE-2022-22718	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Print Sooler, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2022/2016/2012/2008, Windows 11/10/8.1/7. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22718
6	CVE-2022-22000	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Common Log File System Driver, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows Server 2022/2019/2016/2012/2008, Windows 11/10/8.1/7. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22000
7	CVE-2022-21999	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Print Sooler, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows Server 2022/2016/2012/2008, Windows 11/10/8.1/7. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21999

8	CVE-2022-21981	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Common Log File System Driver, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows Server 2019/2012/2008, Windows 11/10/8.1/7. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21981
9	CVE-2022-21996	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows32k, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows 11. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21996
10	CVE-2022-22715	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Named Pipe File System, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows 11/10, Windows Server 2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22715

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng bảo mật nói trên theo hướng dẫn của hãng. Quý đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo tại mục 1 của phụ lục.

3. Tài liệu tham khảo

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

<https://www.zerodayinitiative.com/blog/2022/2/8/the-february2022-security-update-review>

syt_thanhhoa_vt_So Y te Thanh Hoa_18/02/2022_15:41:02