

**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

Hà Nội, ngày tháng năm 2022

V/v lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool

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 786/CATTT-NCSC ngày 01/06/2022 của Cục An toàn thông tin về việc lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool.

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. Hiện Microsoft chưa phát hành bản vá cho lỗ hổng bảo mật nói trên, vì vậy Quý đơn vị cần thực hiện các bước khắc phục thay thế để giảm thiểu nguy cơ tấn công và chờ đến khi bản vá được công bố từ hãng (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 Trị, 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

PHỤ LỤC
THÔNG TIN VỀ LỖ HỔNG BẢO MẬT
CVE-2022-30190

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

1. Thông tin các lỗ hổng bảo mật

- **Mô tả:** Lỗ hổng tồn tại trong Microsoft Windows Support Diagnostic Tool (MSDT) cho phép đối tượng tấn công thực thi mã tùy ý.

- **Điểm CVSS:** 7.8 (Cao)

- **Ảnh hưởng:** Windows Server 2008/2012/2016/2019/2022, Windows 7/8.1/10/11.

2. Hướng dẫn khắc phục

Thời điểm hiện tại hãng chưa phát hành bản vá cho lỗ hổng bảo mật này. Vì vậy, Quý đơn vị cần thực hiện các biện pháp khắc phục thay thế để giảm thiểu nguy cơ tấn công bằng cách vô hiệu hóa giao thức URL MSDT. Cụ thể như sau:

Bước 1: Chạy **Command Prompt** với quyền Admin.

Bước 2: Để sao lưu registry key, chạy lệnh

```
reg export HKEY_CLASSES_ROOT\ms-msdt filename
```

Bước 3: Chạy lệnh

```
reg delete HKEY_CLASSES_ROOT\ms-msdt /f
```

3. Tài liệu tham khảo

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190>

<https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability>

syt_thanhhoa_vt_So Y te Thanh Hoa_29/06/2022 09:30:26