UBND TỈNH TUYÊN QUANG
**SỞ THÔNG TIN VÀ TRUYỀN THÔNG**

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

Số: 616/STTTT-CNTT&BCVT
V/v lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool

*Tuyên Quang, ngày 06 tháng 6 năm 2022*

Kính gửi:
- Văn phòng Đoàn Đại biểu Quốc hội và Hội đồng nhân dân;
- Văn phòng Ủy ban nhân dân tỉnh;
- Các sở, ban, ngành;
- Các tổ chức Chính trị- xã hội;
- Uỷ ban nhân dân các huyện, thành phố.

Căn cứ văn bản số 786/CATTT – NCSC ngày 01/6/2022 của Cục An toàn thông tin về việc lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool, Sở Thông tin và Truyền thông cung cấp thông tin và đưa ra các giải pháp phòng, tránh việc khai thác lỗ hổng bảo mật trong các sản phẩm Microsoft như sau:

**I. Thông tin về lỗ hổng bảo mật trong các sản phẩm Microsoft**

Ngày 30/5/2022, Microsoft đã chính thức công bố về lỗ hổng bảo mật CVE2022-30190 trong Microsoft Support Diagnostic Tool (MSDT), ảnh hưởng đến Microsoft Office phiên bản Office 2013/2016/2019/2021và các phiên bản Professional Plus. Lỗ hổng này cho phép đối tượng tấn công thực thi mã tùy ý; từ đó có quyền xem, thay đổi hoặc xóa dữ liệu,…

(*Thông tin chi tiết các lỗ hổng bảo mật có tại phụ lục kèm theo).*

Lỗ hổng CVE-2022-30190 hay còn có tên gọi "Follina" được phát hiện với những dấu hiệu khai thác đầu tiên từ ngày 12/4/2022 khi sử dụng tài liệu Word độc hại để thực thi mã PowerShell. Thời điểm hiện tại Microsoft vẫn chưa phát hành bản vá cho lỗ hổng này trong khi mã khai thác của Follina đã được công bố rộng rãi trên Internet; cho thấy mức độ ảnh hưởng của lỗ hổng này rất lớn.

**II. Các giải pháp phòng tránh**

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý cơ quan đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông đề nghị các sở, ban, ngành, Ủy ban nhân dân các huyện, thành phố triển khai thực hiện:

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.

3.Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ais@mic.gov.vn.

Trân trọng./.

***Nơi nhận:***
- Như trên;
- Ban Giám đốc sở (báo cáo);
- Các phòng, đơn vị trực thuộc sở;
- Lưu: VT, CNTT&BCVT.

**KT. GIÁM ĐỐC**
**PHÓ GIÁM ĐỐC**

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TUYÊN QUANG

**Nguyễn Văn Hiến**

**Phụ lục**

**Thông tin về lỗ hổng bảo mật CVE-2022-30190**

*(Kèm theo Công văn số* 616 */* STTTT-CNTT&BCVT *ngày 06/ 6/2022 của Sở Thông tin và Truyền thông)*

**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

**2. 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/