SỞ THÔNG TIN VÀ TRUYỀN THÔNG THANH HÓA
TRUNG TÂM CNTT&TT

Số: 78 /TTCNTT&TT-QTHT
V/v lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool

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

Thanh Hoá, ngày 06 tháng 6 năm 2022

Kính gửi:
- Văn Phòng Tỉnh ủy;
- Văn Phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn Phòng UBND tỉnh;
- Các sở, ban, ngành cấp tỉnh;
- UBND các huyện, thị xã, thành phố;
- Các tổ chức đoàn thể chính trị cấp tỉnh;
- Các doanh nghiệp viễn thông, CNTT trên địa bàn tỉnh.

Căn cứ Công văn số 786/CATTT-NCSC ngày 01/6/2022 về lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool của Cục An toàn thông tin, Bộ Thông tin và Truyền thông. Theo đó, ngày 30/5/2022, hãng phần mềm Microsoft đã chính thức công bố về lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool (MSDT), ảnh hưởng đến bộ phần mềm soạn thảo văn bản Microsoft Office phiên bản 2013/2016/2019/2021 và các phiên bản Professional Plus.

Thông qua việc khai thác lỗ hổng này cho phép đối tượng tấn công có thể thực thi mã điều khiển hệ thống bị tấn công một cách tùy ý; từ đó có quyền xem, thay đổi hoặc xóa dữ liệu. Hiện nay, hãng Microsoft vẫn chưa phát hành bản vá cho lỗ hổng này trong khi mã khai thác lỗ hổng bảo mật CVE-2022-30190 đã được công bố rộng rãi trên Internet; cho thấy mức độ ảnh hưởng của lỗ hổng này rất lớn.

Để tăng cường chủ động phòng ngừa các rủi ro mất an toàn thông tin tại các hệ thống thông tin của các cơ quan, địa phương do hình thức tấn công trên có thể xảy ra, Trung tâm Công nghệ thông tin và Truyền thông đề nghị các cơ quan, đơn vị chỉ đạo các bộ phận, cá nhân thực hiện những nội dung sau:

1. Kiểm tra, rà soát, xác định máy tính đang sử dụng tại các hệ thống thông tin của cơ quan, đơn vị có sử dụng hệ điều hành Windows có các phiên bản bị ảnh hưởng. Hiện hãng 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. Hướng dẫn kỹ thuật cách thức thực hiện chi tiết đối với lỗ hổng bảo mật tại địa chỉ: https://attt.thanhhoa.gov.vn

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 quá trình thực hiện, nếu gặp khó khăn, vướng mắc về kỹ thuật liên quan đến các nội dung, công việc trên đề nghị liên hệ với Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa (cơ quan thường trực của Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh) để phối hợp hỗ trợ, xử lý.

Điện thoại: (0237)3718.699

Thư điện tử: ungcuusuco@thanhhoa.gov.vn

Xin trân trọng cảm ơn./.

Nơi nhận:
- Như kính gửi;
- Sở TT&TT (để b/c);
- PGĐ Sở Nguyễn Văn Tước (để b/c);
- Giám đốc Trung tâm (để b/c);
- Lưu: VT, QTHT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG TỈNH THANH HÓA
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Trần Ngọc Hưng

Phụ lục: Thông tin các lỗ hổng bảo mật

(Kèm theo công văn số /TTCNTT&TT-QTHT ngày tháng năm 2022 của Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa)

1. Thông tin các lỗ hổng bảo mật

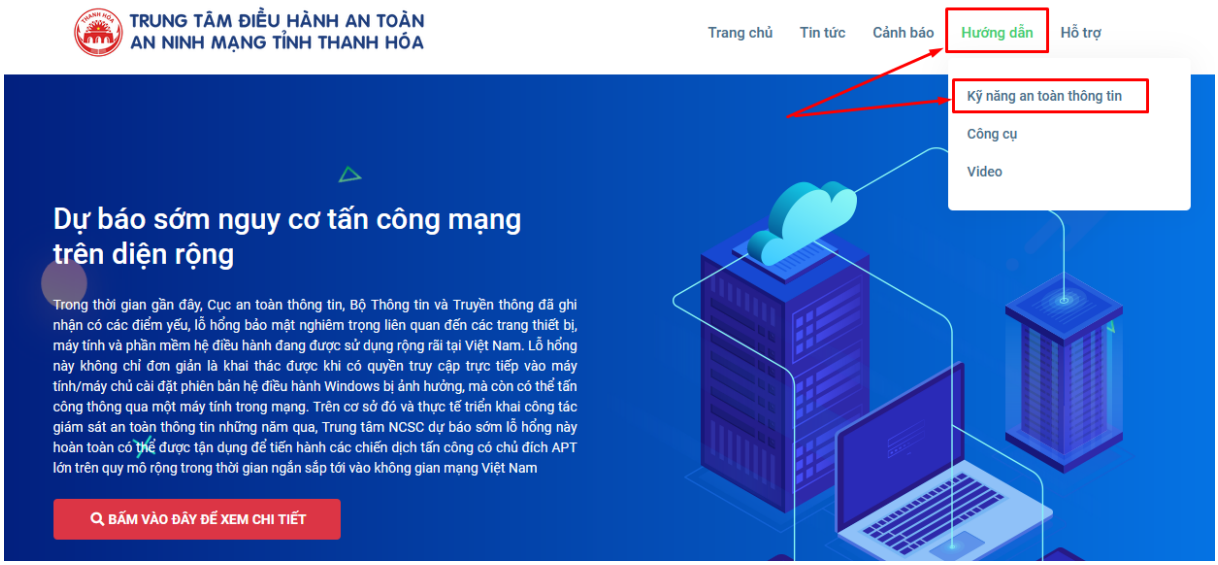
- **Mô tả:** Lỗ hổng tồn tại trong Microsoft Windows Support Diagnostic Tool (MSDT) cho phép đối tượng tấn công thực thi mã tùy ý.

- **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

Hướng dẫn chi tiết khắc phục các lỗ hổng bảo mật trên tại địa chỉ: **https://attt.thanhhoa.gov.vn** (*Mục Hướng dẫn → Kỹ năng An toàn thông tin*)



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/