UBND TỈNH NGHỆ AN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 867 /STT&TT-CNTT
V/v cảnh báo lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool

Nghệ An, ngày 02 tháng 6 năm 2022

Kính gửi:
- Các Sở, ban, ngành cấp tỉnh;
- UBND các huyện, thành phố, thị xã;
- Các tổ chức Chính trị – Xã hội;
- Phòng cơ yếu, CNTT – Văn phòng Tỉnh uỷ.

Ngày 01/06/2022, Cục An toàn thông tin, Bộ Thông tin và Truyền thông đã có công văn số 786/CATTT-NCSC về lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool. Theo văn bản này, Cục An toàn thông tin cung cấp thông tin:

Ngày 30/5/2022, Microsoft đã chính thức công bố về lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool (MSDT), ảnh hưởng đến Microsoft Office phiên bản Office 2013/2016/2019/2021 và 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,…

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.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan nhà nước cuả tỉnh, Sở Thông tin và Truyền thông đề nghị Lãnh đạo các đơn vị chỉ đạo các đơn vị, cá nhân có liên quan thuộc phạm vi quản lý thực hiện một số khuyến nghị của Bộ Thông tin và Truyền thông như sau:

1. Các giải pháp kỹ thuật khuyến nghị

- 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).

- 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.

2. Đề nghị Phòng cơ yếu, CNTT – Văn phòng Tỉnh uỷ tham mưu văn bản thông báo cho các tổ chức cơ sở Đảng để biết và thực hiện.

3. Đề nghị Cổng Thông tin điện tử Nghệ An

- Đăng tải toàn văn nội dung công văn 786/CATTT-NCSC của Cục An toàn thông tin, Bộ Thông tin và Truyền thông lên Cổng thông tin điện tử tỉnh Nghệ An.

- Tổ chức kiểm tra, rà soát, kịp thời có phương án xử lý đối với các hệ thống hiện đang chủ trì quản trị kỹ thuật.

- Bố trí cán bộ kỹ thuật thường xuyên theo dõi hệ thống, hỗ trợ người sử dụng khi có nhu cầu.

4. Giao Trung tâm CNTT&TT Nghệ An

- Tổ chức kiểm tra, rà soát, kịp thời có phương án xử lý đối với các hệ thống hiện đang chủ trì quản trị kỹ thuật, đặc biệt hệ thống mạng máy tính của Sở Thông tin và Truyền thông.

- Bố trí đủ cán bộ thuộc bộ phận ứng cứu sự cố sẵn sàng thực hiện nhiệm vụ khi có điều động.

- Nghiên cứu giải pháp hỗ trợ các đơn vị khắc phục sự cố khi có yêu cầu.

5. Viễn thông Nghệ An (nhà cung cấp dịch vụ hệ thống VNPT-IOffice và VNPT-IGate)

Tuân thủ các quy định pháp lý hiện hành và các điều khoản thuộc hợp đồng thuê dịch vụ có liên quan đến công tác an toàn thông tin để đảm bảo hoạt động ổn định, an toàn các hệ thống: Cổng dịch vụ công trực tuyến tỉnh Nghệ An; Hệ thống phần mềm quản lý văn bản VNPT IOffice.

Mọi thông tin cần hỗ trợ đề nghị Quý cơ quan, tổ chức, cá nhân liên hệ: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại 02432091616, thư điện tử: ais@mic.gov.vn./.

Nơi nhận:
- Như trên;
- Cục ATTT, Bộ TT&TT (b/c);
- UBND tỉnh Nghệ An (b/c);
- VNPT Nghệ An;
- Ban Giám đốc Sở;
- Cổng TTĐT Nghệ An;
- TrT. CNTT&TT Nghệ An;
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG TỈNH NGHỆ AN

Phan Nguyên Hào

Phụ lục Thông tin lỗ hổng bảo mật

(Kèm theo Công văn số /STT&TT-CNTT ngày 01/06/2022 của Sở Thông tin và Truyền thông tỉnh Nghệ An)

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/