UBND TỈNH THỪA THIÊN HUẾ
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1295/STTTT-IOC
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

Thừa Thiên Huế, ngày 07 tháng 6 năm 2022

Kính gửi:
- Các cơ quan chuyên môn thuộc UBND tỉnh;
- Các đơn vị sự nghiệp thuộc tỉnh;
- UBND các huyện, thị xã và thành phố Huế;
- Các cơ quan, đơn vị, tổ chức khác có kết kết mạng WAN.

Sở Thông tin và Truyền thông nhận được Công văn số 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.

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,…

Thông tin chi tiết 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.

Nhằm đảm bảo an toàn thông tin, không để tin tặc tận dụng lỗ hổng bảo mật để tiến hành các cuộc vào hệ thống thông tin tập trung của tỉnh, Sở Thông tin và Truyền thông kính đề nghị quý đơn vị chủ động thực hiện các biện pháp sau:

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 Sở Thông tin và Truyền thông và các cơ quan chức năng về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

Trong trường hợp cần hỗ trợ, quý đơn vị liên hệ đầu mối hỗ trợ của Sở Thông tin và Truyền thông:

- đ/c Hoàng Diên Kỷ; điện thoại: 0906 760 759;

email: hdky.stttt@thuathienhue.gov.vn

- đ/c La Thức; điện thoại: 0772 428 218;

email: lthuc.stttt@thuathienhue.gov.vn

Phòng Giám sát, điều hành an toàn, an ninh mạng - Trung tâm Giám sát, điều hành đô thị thông minh.

Trân trọng./.

Nơi nhận:
- Như trên;
- UBND tỉnh (để bc);
- PA05-Công an tỉnh;
- BGĐ Sở;
- Lưu: VT, P.CNTT, IOC.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Nguyễn Dương Anh

Phụ lục

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

(Kèm theo Công văn số 1295/STTTT-IOC ngày 07/ 6 /2022 của Sở Thông tin và Truyền thông tỉnh Thừa Thiên Huế)

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/