UBND TỈNH PHÚ YÊN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 590 /STTTT-CNTT

V/v triển khai Công văn số 786/CATTT-NCSC về lỗ hổng bảo mật CVE-2022-30190

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

Phú Yên, ngày 06 tháng 6 năm 2022

Kính gửi:
- Hội đồng nhân dân tỉnh;
- Các Sở, ban, ngành;
- Mặt trận, các Hội, Đoàn thể;
- Hội đồng nhân dân các huyện, thị xã, thành phố;
- UBND các huyện, thị xã, thành phố;
- Các tổ chức chính trị - xã hội tỉnh;
- Các Doanh nghiệp nhà nước (cấp tỉnh).

Tiếp nhận Công văn số 786/CATTT-NCSC ngày 01/6/2022 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông V/v lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool, theo đó lỗ 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,…

Để đảm bảo an toàn thông tin cho hệ thống thông tin của các đơn vị, Sở Thông tin và Truyền thông đề nghị:

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 lỗ hổng và hướng dẫn khắc phục như phụ lục đính kèm)*.

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.

Sở Thông tin và Truyền thông Phú Yên thông báo đến Quý cơ quan, đơn vị nghiên cứu thực hiện./.

Nơi nhận:
- Như trên;
- Giám đốc, các PGĐ Sở;
- Phòng VH&TT các huyện, tx, tp;
- Trung tâm CNTT-TT;
- Lưu: VT, CNTT (D).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG TỈNH PHÚ YÊN

Lê Tỷ Khánh

PHỤ LỤC

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

(Kèm theo Công văn số 786/CATTT-NCSC ngày 01/6/2022)

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/
