UBND TỈNH TRÀ VINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1430/STTTT-BCVTCNTT
V/v cảnh báo nguy cơ thực thi mã độc từ xa trên hệ điều hành Windows do lỗ hổng trong Windows Network File System (CVE-2022-22029)

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

Trà Vinh, ngày 15 tháng 7 năm 2022

Kính gửi:
- Các Sở, Ban, ngành tỉnh (3 hệ);
- Công an tỉnh;
- UBND các huyện, thị xã, thành phố.

Trong quá trình vận hành, giám sát an toàn thông tin của Trung tâm Công nghệ thông tin và Truyền thông qua hệ thống giám sát của Trung tâm điều hành an ninh mạng (SOC) phát hiện lỗ hổng thực thi mã độc từ xa trong Windows Network File System (CVE-2022022029), lỗ hổng này có mức ảnh hưởng rất nghiêm trọng, nếu khai thác lỗ hổng thành công tin tặc có thể thực thi mã tùy ý trên máy chủ.

Để ngăn ngừa nguy cơ tấn công nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị, góp phần đảm bảo an toàn thông tin cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị tiến hành kiểm tra, rà soát, xác định máy chủ sử dụng hệ điều hành có khả năng bị ảnh hưởng và thực hiện việc cập nhật bản vá Patch Tuesday tháng 7/2022 của Microsoft, các cơ quan, đơn vị tham khảo cách khắc phục tại phụ lục thông tin và hướng dẫn khắc phục lỗ hổng *(kèm phụ lục)*.

Trong quá trình thực hiện, nếu cần hỗ trợ, các cơ quan, đơn vị liên hệ Sở Thông tin và Truyền thông *(qua Phòng Bưu chính, Viễn thông - Công nghệ thông tin, điện thoại: 0294 3850 853)* để được hướng dẫn./.

Nơi nhận:
- Như trên;
- BGĐ Sở (b/c);
- Công an tỉnh;
- Trung tâm CNTT&TT(t/h);
- Lưu: VT, BCVTCNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TRÀ VINH

Bùi Thống Nhứt

PHỤ LỤC

THÔNG TIN VÀ HƯỚNG DẪN KHẮC PHỤC LỖ HỔNG

(Kèm Công văn số /STTTT-BCVTCNTT ngày tháng 7 năm 2022 của Sở Thông tin và Truyền thông)

1. Thông tin về lỗ hổng bảo mật

a) Mức độ: CAO

b) Mô tả: Lỗ hổng tồn tại trong mô-đun chia sẻ tệp qua mạng của hệ điều hành Windows (Windows Network File System), cho phép đối tượng tấn công thực thi mã tùy ý trên máy chủ nạn nhân.

c) Ảnh hưởng:

- Máy chủ sử dụng hệ điều hành Windows các phiên bản:

° Windows Server 2012 R2 (Server Core installation).

° Windows Server 2012 R2.

° Windows Server 2012 (Server Core installation).

° Windows Server 2012.

° Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation).

° Windows Server 2008 R2 for x64-based Systems Service Pack 1.

° Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation).

° Windows Server 2008 for x64-based Systems Service Pack 2.

° Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation).

° Windows Server 2008 for 32-bit Systems Service Pack 2.

° Windows Server 2016 (Server Core installation).

° Windows Server 2016.

° Windows Server, version 20H2 (Server Core Installation).

° Windows Server 2022 (Server Core installation).

° Windows Server 2022.

° Windows Server 2019 (Server Core installation).

° Windows Server 2019.

- Máy chủ chưa cài đặt bản vá Patch Tuesday tháng 07/2022 hoặc chưa cài đặt bản vá trực tiếp của Microsoft cho lỗ hổng.

2. Hướng dẫn khắc phục

a) Thực hiện cập nhật bản vá Patch Tuesday tháng 7/2022 của Microsoft hoặc bản vá trực tiếp cho lỗ hổng tại địa chỉ: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22029

b) Trường hợp chưa thể cập nhật, cơ quan có thể áp dụng phương án khắc phục tạm thời sau đây:

- Bước 1: tắt dịch vụ NFSV3 bằng lệnh:

Set-NfsServerConfiguration -EnableNFSV3 $false

- Bước 2: khởi động lại NFS server hoặc khởi động lại máy chủ.

- Bước 3: Kiểm tra dịch vụ đã được tắt sử dụng lệnh:

Get-fsServerConfiguration

Nếu kết quả có dòng EnableNFSV3: False thì dịch vụ đã được tắt.