

Số: 134 /TTCNTT-KTHT  
V/v Cảnh báo lỗ hổng trên dịch vụ  
Remote Desktop

Hà Nội, ngày 06 tháng 06 năm 2019

Kính gửi: Các đơn vị trực thuộc Bộ

Ngày 14/5/2019, Microsoft đã cảnh báo về nguy cơ khai thác và phát tán mã độc có thể dẫn tới một đại dịch tương tự WannaCry thông qua việc khai thác lỗ hổng CVE-2019-0708 trên dịch vụ Remote Desktop (dịch vụ cho phép điều khiển máy tính từ xa trên các hệ điều hành Windows). Lỗ hổng này được các chuyên gia gọi là BlueKeep.

Theo Microsoft, bản thân dịch vụ Microsoft không dễ bị tấn công, tuy nhiên lỗ hổng này xảy ra trước khi xác thực và không yêu cầu người dùng tương tác cũng có thể cài cắm mã độc vào máy tính người dùng. Do vậy đối tượng tấn công hoàn toàn có thể khai thác và lây lan mã độc tự động tương tự như WannaCry đã thực hiện vào năm 2017.

Lỗ hổng này ảnh hưởng đến các hệ điều hành Windows 7, Windows Server 2008 R2, Windows Server 2008. Hệ điều hành đã bị ngừng hỗ trợ (XP và Server 2003, Vista) cũng bị ảnh hưởng.

Do mức độ nguy hiểm của lỗ hổng, Microsoft cũng đã phát hành bản vá bảo mật cho tất cả hệ điều hành bị ảnh hưởng bao gồm cả hệ điều hành bị ngừng hỗ trợ bản vá bảo mật.

Việt Nam có 16.876 máy tính đang mở cổng dịch vụ Remote Desktop trên Internet. Đến ngày 23/5/2019 vẫn còn rất nhiều (>2000 máy) máy chưa được vá lỗ hổng bảo mật đồng thời đang cho phép truy cập trực tiếp từ Internet. Khi một trong những máy tính này bị tấn công, lây nhiễm mã độc thì những máy khác trong cùng một vùng mạng rất dễ bị ảnh hưởng.

Nhằm bảo đảm an toàn thông tin, phòng tránh các nguy cơ tấn công mạng, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Trung tâm Công nghệ thông tin đề nghị quản trị viên tại tất cả các đơn vị và người dùng kiểm tra và cập nhật ngay bản vá bảo mật cho các hệ điều hành đang sử dụng, đặc biệt bản vá cho lỗ hổng CVE-2019-0708. Sau khi cập nhật bản vá cần khởi động lại hệ điều hành.

Đặc biệt đối với đơn vị có thiết bị quảng cáo, thiết bị điều khiển sử dụng hệ điều hành Windows đang lắp đặt ở địa điểm công cộng cần phải đặc biệt lưu ý để không bị lợi dụng phát tán những hình ảnh, nội dung trái phép ảnh hưởng đến không gian mạng Việt Nam.

Thông tin bản vá:

- Windows 7/Server 2008: <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708>

- Windows XP/Server 2003/Vista: <https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708>

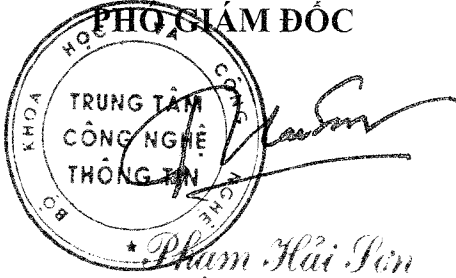
Thông tin liên hệ Trung tâm Công nghệ thông tin, tầng 5, số 113 Trần Duy Hưng, Cầu Giấy, Hà Nội; số điện thoại: 024.3943.9060; thư điện tử [phongktht@most.gov.vn](mailto:phongktht@most.gov.vn).

Trân trọng./.

**Nơi nhận:**

- Như trên;
- Thứ trưởng Bùi Thế Duy (đề b/c);
- Lưu: TTCNTT.

KT. GIÁM ĐỐC  
PHỤ GIÁM ĐỐC



TRUNG TÂM  
CÔNG NGHỆ  
THÔNG TIN

\*Phạm Hải Sơn