UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 330 /STTTT-TTGSĐH
Về việc cảnh báo lỗ hổng bảo mật có mức ảnh hưởng Cao trong các sản phẩm Microsoft công bố tháng 3/2022

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

Tây Ninh, ngày 11 tháng 3 năm 2022

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các cơ quan tham mưu, giúp việc Tỉnh ủy;
- Mặt trận Tổ quốc và các Đoàn thể chính trị - xã hội;
- Các Sở, ban, ngành tỉnh;
- Các huyện, thị, thành ủy;
- UBND các huyện, thị xã, thành phố.

Thực hiện theo Công văn số 315/CATTT-NCSC của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 3/2022 *(Thông tin chi tiết phụ lục)*.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin cho người dùng, đơn vị và toàn bộ hệ thống của tỉnh, Sở Thông tin và Truyền thông đề nghị các đơn vị, địa phương thực hiện gấp các công việc cụ thể như sau:

1. Kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời theo hướng dẫn tại phụ lục để tránh nguy cơ bị tấn công.

2. Tăng cường kiểm tra, giám sát hệ thống mạng của đơn vị, địa phương, khi có phát hiện hoạt động tấn công mạng, đề nghị liên hệ Sở Thông tin và Truyền thông để phối hợp xử lý kịp thời.

Thông tin liên quan đề nghị liên hệ Ông Vương Duy Thanh - Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung; Điện thoại: 0932624462.

Trân trọng./.

Nơi nhận:
- Như trên;
- GĐ Sở (b/c);
- Lưu: VT, TTGSĐH, P.CNTTBCVT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TÂY NINH

Nguyễn Trung Hiếu

PHỤ LỤC
Thông tin các lỗ hổng nghiêm trọng trong các sản phẩm Microsoft công bố tháng 3/2022

1.Thông tin lỗ hổng bảo mật

- Mô tả:

+ 02 lỗ hổng bảo mật **CVE-2022-21990, CVE-2022-23285** trong Remote Desktop Client cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đã có mã khai thác được công bố rộng rãi trên Internet.

+ Lỗ hổng bảo mật **CVE-2022-24459** trong Windows Fax và Scan Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.

+ Lỗ hổng bảo mật **CVE-2022-24508** trong SMBv3 cho phép đối tượng tấn công thực thi mã từ xa trên Windows SMBv3 Client/Server.

+ Lỗ hổng bảo mật **CVE-2022-23277** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa với tài khoản xác thực hợp lệ.

+ Lỗ hổng bảo mật **CVE-2022-21967** trong Xbox Live Auth Manager for Windows cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.

+ Lỗ hổng bảo mật **CVE-2022-22006** trong HEVC Video Extensions cho phép đối tượng tấn công thực thi mã từ xa.

+ Lỗ hổng bảo mật **CVE-2022-24501** trong cho phép đối tượng tấn công thực thi mã từ xa.

- Ảnh hưởng:

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-21990	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Remote Desktop Client cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21990
2	CVE-2022-23285	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Remote Desktop Client cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022,Windows 10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23285

3	CVE-2022-24459	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng Windows Fax và Scan Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24459
4	CVE-2022-24508	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong trong SMBv3 cho phép đối tượng tấn công thực thi mã từ xa trên Windows SMBv3 Client/Server. - Ảnh hưởng: Windows 10/11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24508
5	CVE-2022-23277	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa với tài khoản xác thực hợp lệ. - Ảnh hưởng: Microsoft Exchange Server 2019/2016/2013.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23277
6	CVE-2022-21967	- Điểm CVSS: 7.0 (Cao) - Lỗ hổng trong trong Xbox Live Auth Manager for Windows cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21967
7	CVE-2022-22006	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong HEVC Video Extensions, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: HEVC Video Extensions.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22006
8	CVE-2022-24501	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong VP9 Video Extensions, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: VP9 Video Extensions.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24501

- Đánh giá mức độ: Đánh giá sơ bộ từ các chuyên gia bảo mật, lỗ hổng này ảnh hưởng đến nhiều thiết bị trên toàn cầu trong đó có cả Việt Nam. Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) đánh giá khả năng các

mã khai thác của các lỗ hổng này sẽ sớm được công khai trên Internet trong thời gian sắp tới.

2. Hướng dẫn khắc phục:

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng bảo mật nói trên theo hướng dẫn của hãng. Quý đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo tại mục 1 của phụ lục.

3. Nguồn tham khảo:

https://msrc.microsoft.com/update-guide/releaseNote/2022-Mar
https://msrc.microsoft.com/update-guide/en-us