UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: /STTTT-TTGSĐH
V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2023

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

Tây Ninh, ngày tháng 02 năm 2023

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 trực thuộc Tỉnh ủy;
- UBND các huyện, thị xã, thành phố.

Thực hiện theo Công văn số 158/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 02/2023 ***(Thông tin chi tiết phụ lục kèm theo)***.

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 sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời 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 - Phó Giám đốc 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);
- P.CNTTBCVT;
- Lưu: VT, TTGSĐH.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Nguyễn Trung Hiếu

PHỤ LỤC
THÔNG TIN CÁC LỖ HỔNG NGHIÊM TRỌNG TRONG CÁC SẢN PHẨM MICROSOFT CÔNG BỐ THÁNG 02/2022

1. Thông tin lỗ hổng bảo mật

a. Mô tả:

- 04 lỗ hổng bảo mật **CVE-2023-21529, CVE-2023-21710, CVE-2023-21707, CVE-2023-21706** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa. Microsoft Exchange Server đã và đang là mục tiêu hàng đầu được các nhóm tấn công có chủ đích (APT) nhắm đến, các đối tượng tấn công khai thác triệt để. Vì vậy, các cơ quan, tổ chức cần đặc biệt chú ý cũng như có kế hoạch để khắc phục và tăng cường giám sát nhằm giảm thiểu và tránh nguy cơ bị tấn công thông qua các lỗ hổng này.
- Lỗ hổng bảo mật **CVE-2023-21716** trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng bảo mật **CVE-2023-21715** trong Microsoft Publisher cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đang bị khai thác trong thực tế.
- 02 lỗ hổng bảo mật **CVE-2023-23376, CVE-2023-21812** trong Windows Common Log File System (CLFS) cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.
- 03 lỗ hổng bảo mật **CVE-2023-21705, CVE-2023-21713, CVE-2023-21528** trong Microsoft SQL Server cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng bảo mật **CVE-2023-21717** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

b. Ảnh hưởng:

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-21529, CVE-2023-21710, CVE-2023-21707, CVE-2023-21706	- Điểm: CVSS: 8.8/7.2 (cao) - Mô tả: lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Exchange Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21529 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21706 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21710 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21707

2	CVE-2023-21716	- Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hổng trong trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Word, Microsoft SharePoint.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21716
3	CVE-2023-21715	- Điểm: CVSS: 7.3 (cao) - Mô tả: lỗ hổng trong Microsoft Publisher cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft 365.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21715
4	CVE-2023-23376, CVE-2023-21812	- Điểm: CVSS: 7.8 (cao) - Mô tả: lỗ hổng trong Windows Common Log File System (CLFS) cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10/11, Windows Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23376 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21812
5	CVE-2023-21705, CVE-2023-21713, CVE-2023-21528	- Điểm: CVSS: 8.8/7.8 (cao) - Mô tả: lỗ hổng trong Microsoft SQL Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: SQL Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21705 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21713 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21528
6	CVE-2023-21717	- Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21717

		tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Microsoft SharePoint.	

c. 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

https://www.zerodayinitiative.com/blog/2023/2/14/the-february-2023-security-update-overview