UBND TỈNH TÂY NINH
**SỞ THÔNG TIN VÀ TRUYỀN THÔNG**

Số: 760 /STTTT-TTGSĐH
V/v cảnh báo lỗ hổng bảo mật có mức ảnh hưởng Cao trong các sản phẩm Microsoft công bố tháng 5/2023

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

*Tây Ninh, ngày 18 tháng 5 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;
- UBND các xã, phường, thị trấn.

Thực hiện theo Công văn số 729/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 5/2023 ***(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 tính sử dụng hệ điều hành Windows và phần mềm 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);
- P.CNTTBCVT;
- Lưu: VT, TTGSĐH.

**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 5/2023**

**1.Thông tin lỗ hổng bảo mật**

**- Mô tả:**

- Lỗ hổng bảo mật **CVE-2023-24955** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

Trong tháng 01 vừa qua, đã có hai lỗ hổng bảo mật được công bố với mã là CVE-2023-21744, CVE-2023-21742 liên quan đến Microsoft SharePoint Server, những lỗ hổng này cho phép đối tượng tấn công thực thi mã từ xa, đã được Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) cảnh báo trong văn bản số 50/CATTT-NCSC về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2023 phát hành ngày 11/01/2023. Qua đó cho thấy, Microsoft SharePoint Server đã và đang là mục tiêu nhắm đến của nhiều đối tượng tấn công mạng nhằm thực hiện các hành động trái phép. Chính vì vậy, các cơ quan, tổ chức cần đặc biệt quan tâm và có phương án khắc phục, xử lý kịp thời nếu bị ảnh hưởng.

- 02 lỗ hổng bảo mật **CVE-2023-29336, CVE-2023-24902** trong Win32k cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật **CVE-2023-29325** trong Windows OLE cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đã được công bố rộng rãi trên Internet.

- Lỗ hổng bảo mật **CVE-2023-24941** trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-24932** trong Secure Boot cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đã được công bố rộng rãi trên Internet.

- Lỗ hổng bảo mật **CVE-2023-29344** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-24953** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

**- Ảnh hưởng:**

| STT | CVE | Mô tả | Link tham khảo |
|---|---|---|---|
| 1 | CVE-2023-24955 | - Điểm: CVSS: 7.2 (cao)<br>- Mô tả: lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft SharePoint Server. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24955 |
| 2 | CVE-2023-29336<br>CVE-2023-24902 | - Điểm: CVSS: 7.8 (cao)<br>- Mô tả: lỗ hổng trong Win32k cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.<br>- Ảnh hưởng: Windows Server, Windows 10,11. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29336<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24902 |
| 3 | CVE-2023-29325 | - Điểm: CVSS: 8.1 (cao)<br>- Mô tả: lỗ hổng trong Windows OLE cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đã được công bố rộng rãi trên Internet.<br>- Ảnh hưởng: Windows Server, Windows 10/11. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29325 |
| 4 | CVE-2023-24941 | - Điểm: CVSS: 9.8 (nghiêm trọng)<br>- Mô tả: lỗ hổng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Windows Server. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24941 |
| 5 | CVE-2023-24932 | - Điểm: CVSS: 6.7 (trung bình)<br>- Mô tả: lỗ hổng trong Secure Boot cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932 |

| | | | |
|---|---|---|---|
| | | này đã được công bố rộng rãi trên Internet.<br>- Ảnh hưởng: Windows Server, Windows 10/11. | |
| 6 | CVE-2023-29344 | - Điểm: CVSS: 7.8 (cao)<br>- Mô tả: lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft Office, Microsoft 365. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29344 |
| 7 | CVE-2023-24953 | - Điểm: CVSS: 7.8 (cao)<br>- Mô tả: lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft Office, Microsoft 365, Microsoft Excel. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24953 |

**- 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/2023/5/8/the-may-2023-security-update-review