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

Số: 1906 /STTTT-TTGSĐH
V/v cảnh báo lỗ hổng bảo mật có mức ảnh hưởng Cao trong các sản phẩm Microsoft công bố tháng 10/2023

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

*Tây Ninh, ngày 26 tháng 10 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 đơn vị ngành dọc;
- 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 1850/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 10/2023 ***(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;
- BGĐ 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 10/2023**

**1.Thông tin lỗ hổng bảo mật**

**- Mô tả:**

- Lỗ hổng an toàn thông tin **CVE-2023-36778** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.

Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin, đã phát hành các văn bản cảnh báo diện rộng về những lỗ hổng ảnh hưởng đến Microsoft Exchange Server. Điều này cho thấy Microsoft Exchange Server vẫn luôn là mục tiêu hàng đầu được các đối tượng tấn công có chủ đích nhắm đến. Vì vậy, để đảm bảo an toàn thông tin cho hệ thống của các cơ quan, tổ chức, Cục An toàn thông tin trân trọng đề nghị các đơn vị rà soát lỗ hổng liên quan đến Microsoft Exchange Server để phát hiện và có phương án xử lý kịp thời, đồng thời tăng cường giám sát nhằm giảm thiểu nguy cơ bị tấn công thông qua các lỗ hổng này.

- Lỗ hổng an toàn thông tin **CVE-2023-36563** trong Microsoft WordPad cho phép đối tượng tấn công thực hiện thu thập thông tin mã băm NTLM của người dùng. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-41763** trong Skype for Business cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

- 02 lỗ hổng an toàn thông tin **CVE-2023-35349, CVE-2023-36697** trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-36434** trong Windows IIS Server cho phép đối tượng tấn công thực hiện leo thang đặc quyền.

**- Ảnh hưởng:**

| STT | CVE | Mô tả | Link tham khảo |
|---|---|---|---|
| 1 | CVE-2023-36778 | - Điểm: CVSS: 8.0 (Cao)<br>- Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft Exchange Server 2016, 2019. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36778 |

| STT | CVE | Mô tả | Link tham khảo |
|---|---|---|---|
| 2 | CVE-2023-36563 | - Điểm: CVSS: 6.5 (Cao)<br>- Mô tả: Lỗ hổng trong Microsoft WordPad cho phép đối tượng tấn công thực hiện thu thập thông tin mã băm NTLM của người dùng. Lỗ hổng hiện đang bị khai thác trong thực tế.<br>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36563 |
| 3 | CVE-2023-41763 | - Điểm: CVSS: 5.3 (Cao)<br>- Mô tả: Lỗ hổng trong Skype for Business cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.<br>- Ảnh hưởng:<br>Skype for Business 2015, 2019. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-41763 |
| 4 | CVE-2023-35349<br>CVE-2023-36697 | - Điểm: CVSS: 9.8 (Nghiêm trọng)<br>- Mô tả: Lỗ hổng trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35349<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36697 |
| 5 | CVE-2023-36434 | - Điểm: CVSS: 9.8 (Cao)<br>- Mô tả: Lỗ hổng trong Windows IIS Server cho phép đối tượng tấn công | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36434 |

| STT | CVE | Mô tả | Link tham khảo |
|---|---|---|---|
| | | thực hiện leo thang đặc quyền.<br>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022 | |

**- 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/2023/10/10/the-october-2023-security-update-review