

UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: /STTTT-TTGSĐH
V/v cảnh báo lỗ hổng bảo mật có mức ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 7/2023

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

Tây Ninh, ngày tháng 7 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 1261/CATTT-NCSC ngày 17/7/2023 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 7/2023 (*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 – Phó Giám đốc Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung; Điện thoại: 0932624462.

Trân trọng./.

Nơi nhận:

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

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

PHỤ LỤC
Thông tin các lỗ hổng nghiêm trọng trong các sản phẩm
Microsoft công bố tháng 7/2023

1. Thông tin lỗ hổng bảo mật

- Mô tả:

- 02 lỗ hổng bảo mật **CVE-2023-33160, CVE-2023-33134** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-36884** trong Office và Windows cho phép đối tượng tấn công thực thi mã từ xa khi người dùng mở tệp tài liệu của Microsoft Office do đối tượng tấn công tạo ra. Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật **CVE-2023-35311** trong Microsoft Outlook 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.

- Lỗ hổng bảo mật **CVE-2023-36874** trong Windows Error Reporting Service 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-2023-32046** trong Windows MSHTML 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-2023-32049** trong Windows SmartScreen 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-2023-32057, CVE-2023-35309** trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa.

- Ảnh hưởng:

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-33160 CVE-2023-33134	- Điểm: CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33160 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33134

2	CVE-2023-36884	<ul style="list-style-type: none"> - Điểm: CVSS: 8.3 (Cao) - Mô tả: lỗ hổng trong Office và Windows HTML cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, 11, Windows Server, Microsoft Office. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884
3	CVE-2023-35311	<ul style="list-style-type: none"> - Điểm: CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). - Ảnh hưởng: Microsoft 365, Microsoft Office, Microsoft Outlook. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35311
4	CVE-2023-36874	<ul style="list-style-type: none"> - Điểm: CVSS: 7.8 (Cao) - Mô tả: lỗ hổng trong Windows Error Reporting Service cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server, Windows 10/11. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36874
5	CVE-2023-32046	<ul style="list-style-type: none"> - Điểm: CVSS: 7.8 (Cao) - Mô tả: lỗ hổng trong Windows MSHTML cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server, Windows 10/11. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046
6	CVE-2023-32049	<ul style="list-style-type: none"> - Điểm: CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). - Ảnh hưởng: Windows Server, Windows 10/11. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32049
7	CVE-2023-32057 CVE-2023-35309	<ul style="list-style-type: none"> - Điểm: CVSS: 9.8 (Nghiêm trọng) 	https://msrc.microsoft.com/update-

	<ul style="list-style-type: none"> - Mô tả: lỗ hổng trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server, Windows 10/11. 	guide/vulnerability/CVE-2023-32057 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35309
--	--	--

- **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 của phụ lục.

3. Nguồn tham khảo:

<https://msrc.microsoft.com/update-guide/>

<https://www.zerodayinitiative.com/blog/2023/7/10/the-july-2023-security-update-review>