UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 2212 /STTTT-TTGSĐH
V/v cảnh báo lỗ hổng bảo mật có mức ảnh hưởng Cao trong các sản phẩm Microsoft công bố tháng 11/2023

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

Tây Ninh, ngày 28 tháng 11 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;
- Các đơn vị ngành dọc.

Thực hiện theo Công văn số 2074/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 11/2023 ***(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 11/2023

1.Thông tin lỗ hổng bảo mật

- Mô tả:

- Lỗ hổng an toàn thông tin **CVE-2023-36397** trong Windows Pragmatic General Multicast cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-36400** trong Windows HMAC Key Derivation cho phép đối tượng tấn công thực hiện leo thang đặc quyền.

- Lỗ hổng an toàn thông tin **CVE-2023-36025** cho phép đối tượng tấn công vượt qua tính năng bảo mật SmartScreen của Windows. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-36038** trong ASP.NET Core cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ (DoS). Thông tin chi tiết về lỗ hổng đã được công bố trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-36439** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-36033** trong Windows Desktop Manager cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-36036** trong Windows Cloud Files Mini Filter Driver cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-36041** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-36413** cho phép đối tượng tấn công vượt qua tính năng bảo mật của Microsoft Office. Thông tin chi tiết về lỗ hổng đã được công bố trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-38177** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa..

- Ảnh hưởng:

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-36397	- Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Pragmatic	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36397

STT	CVE	Mô tả	Link tham khảo
		General Multicast cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022	
2	CVE-2023-36400	- Điểm: CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows HMAC Key Derivation cho phép đối tượng tấn công thực hiện leo thang đặc quyền. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36400
3	CVE-2023-36025	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công vượt qua tính năng bảo mật SmartScreen của Windows. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36025
4	CVE-2023-36038	- Điểm: CVSS: 8.2 (Cao) - Mô tả: Lỗ hổng trong ASP.NET Core cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ (DoS). Thông tin chi tiết về lỗ hổng đã được công bố trong thực tế. - Ảnh hưởng: ASP.NET Core, .NET, Visual Studio 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36038

STT	CVE	Mô tả	Link tham khảo
5	CVE-2023-36439	- Điểm: CVSS: 8.0 (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 2016, 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36439
6	CVE-2023-36033	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows Desktop Manager cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36033
7	CVE-2023-36036	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows Cloud Files Mini Filter Driver cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36036
8	CVE-2023-36041	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Excel, Microsoft Office, Microsoft 365 Apps.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36041

STT	CVE	Mô tả	Link tham khảo
9	CVE-2023-36413	- Điểm: CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công vượt qua tính năng bảo mật của Microsoft Office. Thông tin chi tiết về lỗ hổng đã được công bố trong thực tế. - Ảnh hưởng: Microsoft Office, Microsoft 365 Apps.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36413
10	CVE-2023-38177	- Điểm: CVSS: 6.1 (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 2016, 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38177

- 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/2023/11/14/the-november-2023-security-update-review