UBND TỈNH QUẢNG NGÃI **SỞ THÔNG TIN VÀ TRUYỀN THÔNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 2405 /STTTT-BCVT&CNTT V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 11/2023	*Quảng Ngãi, ngày 23 tháng 11 năm 2023*

Kính gửi:

- Văn phòng: Tỉnh ủy, Đoàn ĐBQH&HĐND, UBND tỉnh;
- Các sở, ban, ngành; Hội, đoàn thể tỉnh;
- UBND các huyện, thị xã, thành phố;
- Báo Quảng Ngãi, Đài Phát thanh và Truyền hình tỉnh;
- Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Công an tỉnh;
- UBND các xã, phường, thị trấn.

Theo cảnh báo của Cục An toàn thông tin tại Công văn số 2074/CATTT-NCSC ngày 22/11/2023 về lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 11/2023, Sở Thông tin và Truyền thông đề nghị lãnh đạo các cơ quan, đơn vị chỉ đạo thực hiện một số biện pháp sau để hạn chế các rủi ro về nguy cơ mất an toàn thông tin, cụ thể:

1. Kiểm tra, rà soát máy chủ, máy trạm có sử dụng hệ điều hành Windows để phát hiện và xử lý kịp thời các máy chủ có khả năng bị ảnh hưởng bởi các lỗ hổng bảo mật sau:

(1) 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.

(2) 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.

(3) 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.

(4) 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.

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

(6) 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.

(7) 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.

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

(9) 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.

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

(Tham khảo thông tin lỗ hổng và cách khắc phục tại Phụ lục Thông tin về lỗ hổng bảo mật kèm theo Công văn này)

2. Khi phát hiện các hệ thống có biểu hiện bị khai thác, tấn công mạng, triển khai ngay các biện pháp xử lý ngăn chặn tấn công trên hệ thống và thông báo về Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi để có các biện pháp hỗ trợ, xử lý kịp thời.

Đề nghị lãnh đạo các cơ quan, đơn vị quan tâm chỉ đạo thực hiện./.

***Nơi nhận*:**
- Như trên;
- Cục An toàn thông tin (báo cáo);
- Phòng VH&TT các huyện, thị xã, thành phố;
- Thành viên Đội ứng cứu sự cố ATTT mạng tỉnh;
- Sở TT&TT: Lãnh đạo Sở, các phòng chuyên môn, TT CNTT&TT;
- Lưu: VT, BCVT&CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH QUẢNG NGÃI

Nguyễn Quốc Huy Hoàng

PHỤ LỤC
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG MICROSOFT
(Kèm theo Công văn số /STTTT-BCVT&CNTT ngày /11/2023 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-36397	- Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Pragmatic 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	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36397
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,	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36025

STT	CVE	Mô tả	Link tham khảo
		2012, 2016, 2019, 2022.	
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
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	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36036

STT	CVE	Mô tả	Link tham khảo
		quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2019, 2022.	
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
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

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng an toàn thông tin 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. Tài liệu tham khảo

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

https://www.zerodayinitiative.com/blog/2023/11/14/the-november-2023-security-update-review