UBND TỈNH THỪA THIÊN HUẾ
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh Phúc

Số: 3249STTTT-IOC
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 11/2023

Thừa Thiên Huế, ngày 22 tháng 11 năm 2023

Kính gửi:
- Văn phòng Tỉnh ủy;
- Các cơ quan chuyên môn thuộc UBND tỉnh;
- Các đơn vị sự nghiệp thuộc tỉnh;
- UBND các huyện, thị xã và thành phố Huế;
- Các cơ quan, đơn vị, tổ chức khác có kết kết mạng WAN.

Ngày 14/11/2023, Microsoft đã phát hành danh sách bản vá tháng 11 với 63 lỗ hổng an toàn thông tin trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý vào các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng sau:

- 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.

Nhằm đảm bảo an toàn thông tin, không để tin tặc tận dụng lỗ hổng bảo mật để tiến hành các cuộc vào hệ thống thông tin tập trung của tỉnh, Sở Thông tin và Truyền thông kính đề nghị quý đơn vị chủ động thực hiện các biện pháp sau:

1. Kiểm tra, rà soát, xác định máy tính/máy chủ sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công *(Thông tin chi tiết các lỗ hổng bảo mật có tại phụ lục kèm theo)*.

2. Triển khai cài đặt 02 giải pháp Bkav Endpoint và EDR cho 100% máy tính tại cơ quan, đơn vị theo các hướng dẫn cài đặt của Sở Thông tin và Truyền thông. *Đây là 02 tiêu chí về An toàn thông tin trong Bộ chỉ số đánh giá, xếp hạng Chuyển đổi số các cấp theo Quyết định số 2263/QĐ-UBND ngày 27/9/2023*
của Uỷ ban nhân dân tỉnh Thừa Thiên Huế về việc Ban hành Bộ chỉ số đánh giá, xếp hạng chuyển đổi số các cấp của tỉnh Thừa Thiên Huế.

3. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; Đồng thời thường xuyên theo dõi kênh cảnh báo của Sở Thông tin và Truyền thông và các cơ quan chức năng về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

Trong trường hợp cần hỗ trợ, quý đơn vị liên hệ đầu mối hỗ trợ của Sở Thông tin và Truyền thông:

- đ/c Hoàng Diên Kỷ; điện thoại: 0906 760 759;

email: hdky.stttt@thuathienhue.gov.vn

- đ/c La Thức; điện thoại: 0772 428 218;

email: lthuc.stttt@thuathienhue.gov.vn

Phòng Giám sát, điều hành an toàn, an ninh mạng - Trung tâm Giám sát, điều hành đô thị thông minh.

Nơi nhận:
- Như trên;
- UBND tỉnh (để bc);
- Công an tỉnh (để p/h);
- BGĐ Sở;
- P.CNTT, HueIOC;
- Lưu: VT.

GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Xuân Sơn

Phụ lục
Thông tin về các lỗ hổng bảo mật Cao và Nghiêm trọng trong sản phẩm Microsoft công bố tháng 11/2023
(Kèm theo Công văn số 3249/STTTT-IOC ngày 22 /11/2023 của Sở Thông tin và Truyền thông tỉnh Thừa Thiên Huế)

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	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36025

STT	CVE	Mô tả	Link tham khảo
		thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 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,	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36033

STT	CVE	Mô tả	Link tham khảo
		Windows Server 2019, 2022.	
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
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

STT	CVE	Mô tả	Link tham khảo
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 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. Tài liệu tham khảo

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

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