

UBND TỈNH THỪA THIÊN HUẾ
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 1748/STTTT-IOC

Thừa Thiên Huế, ngày 30 tháng 6 năm 2023

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2023

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 13/06/2023, Microsoft đã phát hành danh sách bản vá tháng 06 với 69 lỗ hổng bảo mật trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý các lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng sau:

- 02 lỗ hổng bảo mật **CVE-2023-32031, CVE-2023-28310** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.

- 02 lỗ hổng bảo mật **CVE-2023-29357, CVE-2023-33142** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

- 03 lỗ hổng bảo mật **CVE-2023-29363, CVE-2023-32014, CVE-2023-32015** trong Windows Pragmatic General Multicast (PGM) cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-3079** liên quan đến lỗi Type confusion trong JavaScript V8 cho phép đối tượng tấn công có thể thực thi các đoạn mã với quyền của người dùng cục bộ. Lỗ hổng này đang được khai thác trong thực tế.

- 03 lỗ hổng bảo mật **CVE-2023-32029, CVE-2023-33133, CVE-2023-33137** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-33146** trong Microsoft Office 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; cập nhật phần mềm Office trong danh sách 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.

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 Kỳ; điện thoại: 0906 760 759;

email: hdky.sttt@thuathienhue.gov.vn

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

email: lthuc.sttt@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

Nguyễn Xuân Sơn

Phụ lục
Thông tin về các lỗ hổng bảo mật Cao và Nghiêm trọng trong sản phẩm
Microsoft công bố tháng 6/2023

*(Kèm theo Công văn số 1748 /STTTT-IOC ngày 30/6/2023 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-2023-32031 CVE-2023-28310	- Điểm: CVSS: 8.8 (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-2023-32031 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28310
2	CVE-2023-29357 CVE-2023-33142	- Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Microsoft SharePoint Server 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29357 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33142
3	CVE-2023-29363 CVE-2023-32014 CVE-2023-32015	- Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: lỗ hổng trong Windows Pragmatic General Multicast (PGM) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29363 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32014 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32015

STT	CVE	Mô tả	Link tham khảo
4	CVE-2023-3079	<ul style="list-style-type: none"> - Điểm: CVSS: N/A - Mô tả: lỗ hổng trong JavaScript V8 cho phép đối tượng tấn công có thể thực thi các đoạn mã với quyền của người dùng cục bộ. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Edge (Chromium-based) 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3079
5	CVE-2023-32029 CVE-2023-33133 CVE-2023-33137	<ul style="list-style-type: none"> - 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. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32029 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33133 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33137
6	CVE-2023-33146	<ul style="list-style-type: none"> - Điểm: CVSS: 7.8 (cao) - Mô tả: lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft 365. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33146

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/2023/6/13/the-june-2023-security-update-review>