

Số: **614** /STTTT-CNTT-VT

Đồng Nai, ngày **20** tháng 3 năm 2023

V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 3/2023

Kính gửi:

- Các cơ quan đảng, nhà nước trên địa bàn tỉnh;
- Các tổ chức chính trị - xã hội thuộc địa bàn tỉnh;
- Viettel Đồng Nai, VNPT Đồng Nai, Mobifone Đồng Nai;
- Trung tâm Công nghệ thông tin tỉnh Đồng Nai.

Sở Thông tin và Truyền thông nhận văn bản 383/CATTT-NCSC ngày 17/3/2023 của Cục An toàn thông tin về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 3/2023;

Theo văn bản trên, ngày 14/3/2023, Microsoft đã phát hành danh sách bản vá tháng 3 với 74 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:

- Lỗ hổng bảo mật **CVE-2023-23397** trong Microsoft Outlook 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-2023-24880** 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.

- Lỗ hổng bảo mật **CVE-2023-23392** trong HTTP Protocol Stack cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-23415** trong Internet Control Message Protocol (ICMP) cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-23399** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-23400** trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa.

Thông tin chi tiết các lỗ hổng bảo mật có tại phụ lục kèm theo.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát, xác định máy 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 (tham khảo thông tin tại phụ lục kèm theo).

2. 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 các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

3. Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ais@mic.gov.vn hoặc Sở Thông tin và Truyền thông, điện thoại 0251.3810.269, thư điện tử: attt@dongnai.gov.vn.

Trân trọng./.

Nơi nhận:

- Như trên;
- UBND tỉnh (b/c);
- Giám đốc và Phó Giám đốc Sở;
- Lưu: VT, CNTT, Thịnh.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Võ Hoàng Khai

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM
MICROSOFT

(Kèm theo văn bản số **614** /STTTT-CNTT-VT ngày **20** / 3/2023
của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-23397	<ul style="list-style-type: none">- Điểm: CVSS: 9.1 (nghiêm trọng)- Mô tả: lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.- Ảnh hưởng: Microsoft Outlook, Microsoft Office.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397
2	CVE-2023-24880	<ul style="list-style-type: none">- Điểm: CVSS: 5.4 (trung bình)- Mô tả: lỗ hổng 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.- Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24880
3	CVE-2023-23392	<ul style="list-style-type: none">- Điểm: CVSS: 9.8 (nghiêm trọng)- Mô tả: lỗ hổng trong HTTP Protocol Stack cho phép đối tượng tấn công thực thi mã từ xa.- Ảnh hưởng: Windows Server, Windows 11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23392

STT	CVE	Mô tả	Link tham khảo
4	CVE-2023-23415	<ul style="list-style-type: none"> - Điểm: CVSS: 9.8 (ngghiêm trọng) - Mô tả: lỗ hổng trong Internet Control Message Protocol (ICMP) 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-2023-23415
5	CVE-2023-23399	<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 Office, Microsoft Excel, Microsoft 365 . 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23399
6	CVE-2023-23400	<ul style="list-style-type: none"> - Điểm: CVSS: 7.2 (cao) - Mô tả: lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23400

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/2023/3/14/the-march-2023-security-update-review>