

Số: **540** /STTTT-CNTT-VT

Đồng Nai, ngày **13** tháng 3 năm 2023

V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2023

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 50/CATTT-NCSC ngày 11/01/2023 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 01/2023;

Theo văn bản trên, ngày 10/01/2023, Microsoft đã phát hành danh sách bản vá tháng 01 với 98 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-2023-21674** trong Windows Advanced Local Procedure Call (ALPC) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.

- 03 lỗ hổng bảo mật **CVE-2023-21743, CVE-2023-21744, CVE-2023-21742** trong Microsoft SharePoint Server, trong đó **CVE-2023-21743** cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật; 02 lỗ hổng **CVE-2023-21744, CVE-2023-21742** cho phép đối tượng tấn công thực thi mã từ xa.

- 04 lỗ hổng bảo mật **CVE-2023-21763, CVE-2023-21764, CVE-2023-21762, CVE-2023-21745** trong Microsoft Exchange Server, trong đó 02 lỗ hổng **CVE-2023-21763, CVE-2023-21764** cho phép đối tượng tấn công thực hiện nâng cao đặc quyền; 02 lỗ hổng **CVE-2023-21762, CVE-2023-21745** cho phép đối tượng tấn công thực hiện tấn công giả mạo.

- Lỗ hổng bảo mật **CVE-2023-21549** trong Windows Workstation Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã được công bố rộng rãi trên Internet.

- 02 lỗ hổng bảo mật **CVE-2023-21561, CVE-2023-21551** trong Microsoft Cryptographic Services cho phép đối tượng tấn công nâng cao đặc quyền.

- 02 lỗ hổng bảo mật **CVE-2023-21734, CVE-2023-21735** trong Microsoft

Office 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 **540** /STTTT-CNTT-VT ngày **13** / 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-2023-21674	<ul style="list-style-type: none">- Điểm: CVSS: 8.8 (cao)- Mô tả: lỗ hổng trong Windows Advanced Local Procedure Call (ALPC) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.- Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21674
2	CVE-2023-21743, CVE-2023-21744, CVE-2023-21742	<ul style="list-style-type: none">- Điểm: CVSS: 8.8 (cao)- Mô tả: lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass), thực thi mã từ xa.- Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21743 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21744 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21742
3	CVE-2023-21763, CVE-2023-21764, CVE-2023-21762, CVE-2023-21745	<ul style="list-style-type: none">- Điểm: CVSS: 8.0/7.8 (cao)- Mô tả: lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền, tấn công giả mạo (Spoofing).- Ảnh hưởng: Microsoft Exchange Server	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21763 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21764 https://msrc.microsoft.com/update-

		2016/2019.	guide/vulnerability/CVE-2023-21762 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21745
4	CVE-2023-21549	- Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong Windows Workstation Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã được công bố rộng rãi trên Internet. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2012/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21549
5	CVE-2023-21561, CVE-2023-21551	- Điểm: CVSS: 8.8/7.8 (cao) - Mô tả: lỗ hổng trong Microsoft Cryptographic Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21561 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21551
6	CVE-2023-21734, CVE-2023-21735	- 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 LTSC for Mac 2021, Microsoft 365, Microsoft Office 2019 for Mac.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21734 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21735

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/2023/1/10/the-january-2023-security-update-review>