UBND TỈNH ĐỒNG NAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 2991 /STTTT-CĐS
V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 09, 10/2023

Đồng Nai, ngày 20 *tháng* 10 *năm 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 được hướng dẫn 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 09, 10/2023, cụ thể: văn bản số 1664/CATTT-NCSC ngày 21/9/2023 về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 09/2023, văn bản số 1850/CATTT-NCSC ngày 19/10/2023 về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2023.

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, của tỉnh và 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.

Số 01, đường 30/4, phường Thanh Bình, TP. Biên Hòa, tỉnh Đồng Nai.
ĐT: (0251) 3810.269 – https://stttt.dongnai.gov.vn

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./.

Nơi nhận:
- Như trên;
- UBND tỉnh (b/c);
- Ban Giám đốc Sở;
- Thanh tra Sở;
- TT. CNTT tỉnh;
- Lưu: VT, CĐS, Thịnh.

GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH ĐỒNG NAI

Tạ Quang Trường

Phụ lục 01.
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM MICROSOFT (THÁNG 09)

(Kèm theo văn bản số /STTTT-CĐS ngày /10/2023 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-36761	- Điểm: CVSS: 6.2 (Cao) - Mô tả: Lỗ hổng trong Microsoft Word cho phép đối tượng tấn công thu thập thông tin về mã băm NTLM của người dùng. Lỗ hổng này hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Word, Microsoft 365.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36761
2	CVE-2023-29332	- Điểm: CVSS: 7.5 (Nghiêm trọng) - Mô tả: Lỗ hổng trong dịch vụ Microsoft Azure Kubernetes Service cho phép đối tượng tấn công không cần xác thực thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Microsoft Azure Kubernetes Service.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29332
3	CVE-2023-38148	- Điểm: CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Internet Connection Sharing (ICS) cho phép đối tượng tấn công không cần xác thực thực thi mã từ xa khi ICS được kích hoạt. - Ảnh hưởng: Windows 10, Windows 11, Windows	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38148

		Server 2022.	
4	CVE-2023-36802	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Streaming Service Proxy cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng này hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36802
5	CVE-2023-38146	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Windows Themes cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38146
6	CVE-2023-36792 CVE-2023-36793 CVE-2023-36794 CVE-2023-36796	- Điểm: CVSS: 7.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Visual Studio cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft .NET Framework.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36792 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36793 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36794 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36796
7	CVE-2023-36744 CVE-2023-36745 CVE-2023-36756	- 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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36744 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36745 https://msrc.microsoft.com/update-

			guide/vulnerability/CVE-2023-36756

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/2023/9/12/the-september-2023-security-update-review

Phụ lục 02.
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM MICROSOFT (THÁNG 10)
(Kèm theo văn bản số /STTTT-CĐS ngày /10/2023 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng an toàn thông tin

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-36761	- Điểm: CVSS: 6.2 (Cao) - Mô tả: Lỗ hổng trong Microsoft Word cho phép đối tượng tấn công thu thập thông tin về mã băm NTLM của người dùng. Lỗ hổng này hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Word, Microsoft 365.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36761
2	CVE-2023-29332	- Điểm: CVSS: 7.5 (Nghiêm trọng) - Mô tả: Lỗ hổng trong dịch vụ Microsoft Azure Kubernetes Service cho phép đối tượng tấn công không cần xác thực thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Microsoft Azure Kubernetes Service.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29332
3	CVE-2023-38148	- Điểm: CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Internet Connection Sharing (ICS) cho phép đối tượng tấn công không cần xác thực thực thi mã từ xa khi ICS được kích hoạt. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38148
4	CVE-2023-36802	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong	https://msrc.microsoft.com/update-

		Streaming Service Proxy cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng này hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 11.	guide/vulnerability/CVE-2023-36802
5	CVE-2023-38146	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Windows Themes cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38146
6	CVE-2023-36792 CVE-2023-36793 CVE-2023-36794 CVE-2023-36796	- Điểm: CVSS: 7.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Visual Studio cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft .NET Framework.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36792 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36793 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36794 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36796
7	CVE-2023-36744 CVE-2023-36745 CVE-2023-36756	- 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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36744 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36745 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36756

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/2023/9/12/the-september-2023-security-update-review