

Số: /STTTT-CNTTVT
V/v lỗ hổng bảo mật ảnh hưởng cao và
nghiêm trọng trong các sản phẩm
Microsoft công bố tháng 5, 6, 7, 8/2023

Đồng Nai, ngày tháng 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 5, 6, 7, 8/2023, cụ thể: văn bản số 729/CATTT-NCSC ngày 15/5/2023 về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 05/2023, văn bản số 1024/CATTT-NCSC ngày 21/6/2023 về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 06/2023, văn bản số 1261/CATTT-NCSC ngày 17/7/2023 về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 07/2023 và văn bản số 1500/CATTT-NCSC ngày 21/8/2023 về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 08/2023;

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, 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: attn@dongnai.gov.vn/.

Nơi nhận:

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

GIÁM ĐỐC

Tạ Quang Trường

Phụ lục 01.
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG
SẢN PHẨM MICROSOFT (THÁNG 05)
(Kèm theo văn bản số /STTTT-CNTT-VT ngày /8/2023
của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-24955	<ul style="list-style-type: none"> - Điểm: CVSS: 7.2 (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. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24955
2	CVE-2023-29336 CVE-2023-24902	<ul style="list-style-type: none"> - Điểm: CVSS: 7.8 (cao) - Mô tả: lỗ hổng trong Win32k 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: Windows Server, Windows 10,11. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29336 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24902
3	CVE-2023-29325	<ul style="list-style-type: none"> - Điểm: CVSS: 8.1 (cao) - Mô tả: lỗ hổng trong Windows OLE cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đã được công bố rộng rãi trên Internet. - Ảnh hưởng: Windows Server, Windows 10/11. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29325
4	CVE-2023-24941	<ul style="list-style-type: none"> - Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hổng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24941

5	CVE-2023-24932	<ul style="list-style-type: none"> - Điểm: CVSS: 6.7 (trung bình) - Mô tả: lỗ hổng trong Secure Boot cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đã được công bố rộng rãi trên Internet. - Ảnh hưởng: Windows Server, Windows 10/11. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932
6	CVE-2023-29344	<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-2023-29344
7	CVE-2023-24953	<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 365, Microsoft Excel. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24953

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/2023/5/8/the-may-2023-security-update-review>

Phụ lục 02.
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM
MICROSOFT (THÁNG 06)

(Kèm theo văn bản số /STTT-CNTT-VT ngày /8/2023
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-2023-32031 CVE-2023-28310	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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
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. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3079

STT	CVE	Mô tả	Link tham khảo
		- Ảnh hưởng: Microsoft Edge (Chromium-based)	
5	CVE-2023-32029 CVE-2023-33133 CVE-2023-33137	- 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	- 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 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/2023/6/13/the-june-2023-security-update-review>

Phụ lục 03.
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM
MICROSOFT (THÁNG 07)

(Kèm theo văn bản số /STTT-CNTT-VT ngày /8/2023
của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-33160 CVE-2023-33134	<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 thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33160 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33134
2	CVE-2023-36884	<ul style="list-style-type: none"> - Điểm: CVSS: 8.3 (Cao) - Mô tả: lỗ hổng trong Office và Windows HTML cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, 11, Windows Server, Microsoft Office. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884
3	CVE-2023-35311	<ul style="list-style-type: none"> - Điểm: CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). - Ảnh hưởng: Microsoft 365, Microsoft Office, Microsoft Outlook. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35311
4	CVE-2023-36874	<ul style="list-style-type: none"> - Điểm: CVSS: 7.8 (Cao) - Mô tả: lỗ hổng trong Windows Error Reporting Service cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server, Windows 10/11. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36874

5	CVE-2023-32046	<ul style="list-style-type: none"> - Điểm: CVSS: 7.8 (Cao) - Mô tả: lỗ hổng trong Windows MSHTML cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server, Windows 10/11. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046
6	CVE-2023-32049	<ul style="list-style-type: none"> - Điểm: CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). - Ảnh hưởng: Windows Server, Windows 10/11. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32049
7	CVE-2023-32057 CVE-2023-35309	<ul style="list-style-type: none"> - Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Message Queuing 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-2023-32057 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35309

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/2023/7/10/the-july-2023-security-update-review>

Phụ lục 04.
THÔNG TIN VỀ CÁC LỖ HỔNG AN TOÀN THÔNG TIN
TRONG SẢN PHẨM MICROSOFT (THÁNG 08)
(Kèm theo văn bản số /STTT-CNTTVT ngày /8/2023
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-2023-38181	<ul style="list-style-type: none"> - Điểm: CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện tấn công Spoofing. - Ảnh hưởng: Exchange Server 2016/2019. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38181
2	CVE-2023-21709	<ul style="list-style-type: none"> - Điểm: CVSS: 9.8 (được Microsoft đánh giá là Cao) - Mô tả: lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Exchange Server 2016/2019. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21709
3	CVE-2023-35368 CVE-2023-38185 CVE-2023-35388 CVE-2023-38182	<ul style="list-style-type: none"> - Điểm: CVSS: 8.0/8.8 (Cao) - Mô tả: lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Exchange Server 2016/2019. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35368 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38185 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35388 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38182

STT	CVE	Mô tả	Link tham khảo
			2023-38182
4	CVE-2023-35385 CVE-2023-36910 CVE-2023-36911	<ul style="list-style-type: none"> - Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10/11, Windows Server. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35385 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36910 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911
5	CVE-2023-29328 CVE-2023-29330	<ul style="list-style-type: none"> - Điểm: CVSS: 8.8 (được Microsoft đánh giá là Nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Teams cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Teams dành cho iOS, Mac, Android, Desktop 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29328 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29330
6	CVE-2023-36895	<ul style="list-style-type: none"> - Điểm: CVSS: 7.8 (được Microsoft đánh giá là Nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft 365 Apps for Enterprise. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36895
7	CVE-2023-36896	<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, Office, Office LTSC, 365 Apps. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36896

STT	CVE	Mô tả	Link tham khảo
8	CVE-2023-35371	<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, Office LTSC, 365 Apps. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35371

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/2023/8/8/the-august-2023-security-update-review>