

Số: /CATTT-NCSC
V/v lỗ hổng an toàn thông tin ảnh hưởng
cao và nghiêm trọng trong các sản phẩm
Microsoft công bố tháng 04/2024

Hà Nội, ngày tháng năm 2024

Kính gửi:

- Đơn vị chuyên trách về CNTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; các Ngân hàng TMCP; các tổ chức tài chính;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

Ngày 09/4/2024, Microsoft đã phát hành danh sách bản vá tháng 04 với 147 lỗ hổng an toàn thông tin trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý vào các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng sau:

- Lỗ hổng an toàn thông tin **CVE-2024-20678** trong Remote Procedure Call Runtime (RPC) cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-29988** trong SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo vệ.
- **03** lỗ hổng an toàn thông tin **CVE-2024-21322, CVE-2024-21323, CVE-2024-29053** trong Microsoft Defender for IoT cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-20670** trong Outlook for Windows làm lộ lọt NTML hash, cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing).
- Lỗ hổng an toàn thông tin **CVE-2024-26256** trong thư viện nguồn mở libarchive cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-26257** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.
- **07** lỗ hổng an toàn thông tin **CVE-2024-26221, CVE-2024-26222, CVE-2024-26223, CVE-2024-26224, CVE-2024-26227, CVE-2024-26231, CVE-2024-26233** trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-26234** trong Proxy Driver cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing).

Thông tin chi tiết các lỗ hổng an toàn thông tin xem 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 không gian mạng Việt Nam, Cục An toàn thông tin khuyến nghị Quý Đơn vị thực hiện:

1. Kiểm tra, rà soát, xác định máy tính 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: ncsc@ais.gov.vn.

Trân trọng./.

Nơi nhận:

- Như trên;
- Thứ trưởng Phạm Đức Long (đề b/c);
- Cục A05, Bộ Công an;
- Bộ Tư lệnh 86, Bộ Quốc phòng;
- Ban Cơ yếu Chính phủ;
- Đơn vị chuyên trách về CNTT/ATTT của: Văn phòng Trung ương Đảng; Văn phòng Quốc hội; Văn phòng Chủ tịch nước; Tòa án Nhân dân tối cao; Viện Kiểm sát Nhân dân tối cao; Kiểm toán Nhà nước; Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam
- Các Cục: Viễn thông, Bưu điện Trung ương;
- Các Trung tâm: TTTT, VNNIC;
- Cục trưởng (đề b/c);
- Các Phó Cục trưởng;
- P. ATHTTT, VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

**KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG**

Trần Đăng Khoa

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG AN TOÀN THÔNG TIN
TRONG SẢN PHẨM MICROSOFT

(Kèm theo Công văn số /CATT-NCSC ngày / /2024
của Cục An toàn thông tin)

1. Thông tin các lỗ hổng an toàn thông tin

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-20678	<ul style="list-style-type: none"> - Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Remote Procedure Call Runtime (RPC) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2008, 2012, 2016, 2019, 2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20678
2	CVE-2024-29988	<ul style="list-style-type: none"> - Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2019, 2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29988
3	CVE-2024-21322 CVE-2024-21323 CVE-2024-29053	<ul style="list-style-type: none"> - Điểm: CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Defender for IoT cho phép đối tượng tấn công thực thi mã từ xa. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21322 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21323 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29053

		- Ảnh hưởng: Microsoft Defender for IoT.	
4	CVE-2024-20670	- Điểm: CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng trong Outlook for Windows làm lộ lọt NTML hash, cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). - Ảnh hưởng: Outlook for Windows.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20670
5	CVE-2024-26256	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong thư viện nguồn mở libarchive cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 11; Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26256
6	CVE-2024-26257	- 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 365 Apps for Enterprise, Microsoft Office LTSC for Mac.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26257

7	<p>CVE-2024-26221 CVE-2024-26222 CVE-2024-26223 CVE-2024-26224 CVE-2024-26227 CVE-2024-26231 CVE-2024-26233</p>	<p>- 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 2016, 2019, 2022.</p>	<p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26221 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26222 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26223 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26224 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26227 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26231 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26233</p>
8	<p>CVE-2024-26234</p>	<p>- Điểm: CVSS: 6.7 (Cao) - Mô tả: Lỗ hổng trong Proxy Driver cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2008, 2012, 2016, 2019, 2022.</p>	<p>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26234</p>

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/2024/4/9/the-april-2024-security-updates-review>