

Số: /TTCNTT-HTATT  
V/v lỗ hổng an toàn thông tin ảnh hưởng  
cao và nghiêm trọng trong các sản phẩm  
Microsoft công bố tháng 9, 10/2024

Hà Nội, ngày tháng 10 năm 2024

Kính gửi: Các đơn vị trực thuộc Bộ  
(Danh sách kèm theo)

Ngày 08/10/2024, Microsoft đã phát hành danh sách bản vá tháng 09 và tháng 10/2024 với **121 lỗ hổng an toàn thông tin** gồm có **117 lỗ hổng an toàn thông tin** trong các sản phẩm của hãng Microsoft và **04 lỗ hổng an toàn thông tin** trong các sản phẩm thuộc bên thứ ba có ảnh hưởng tới Microsoft. 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:

Các lỗ hổng này có mức độ ảnh hưởng **Cao** và **Nghiêm trọng**, có thể bị đối tượng tấn công khai thác để thực hiện các hành vi trái phép, gây ra nguy cơ mất an toàn thông tin và ảnh hưởng đến các hệ thống thông tin của cơ quan, tổ chức và doanh nghiệp.

Lỗ hổng an toàn thông tin tồn tại trên một số sản phẩm của Microsoft như: Microsoft Office and Components; Windows Hyper-V; Windows DHCP Server; Microsoft Streaming Service; Microsoft Management Console; Windows MSHTML Platform; Microsoft Dynamics 365 (on-premise); Windows; Microsoft Office; Azure; .NET và Visual Studio; OpenSSH cho Windows; Power BI; Windows Hyper-V; Windows Mobile Broadband;.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị và người sử dụng, Trung tâm Công nghệ thông tin khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát, xác định máy sử dụng sản phẩm của Microsoft 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.

Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Hạ tầng và an toàn thông tin, 113 Trần Duy Hưng, Trung

Hòa, Cầu Giấy, Hà Nội; số điện thoại: 024.39439060; địa chỉ thư điện tử: phongktht@most.gov.vn.

Trân trọng./.

***Nơi nhận:***

- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Giám đốc (để b/c);
- Cổng thông tin điện tử của Bộ (để đăng tải);
- Lưu: VT.

**KT. GIÁM ĐỐC  
PHÓ GIÁM ĐỐC**

**Ngô Minh Phước**

**Phụ lục**  
**THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG**  
**SẢN PHẨM MICROSOFT**  
(Kèm theo Công văn số /TTCNTT-HTATTT ngày / 10 /2024  
của Trung tâm Công nghệ thông tin)

**1. Thông tin các lỗ hổng bảo mật**

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-43491	<p>- Điểm CVSS: 9.8 (Nghiêm trọng)- Mô tả: Lỗ hổng trong Microsoft Windows Update cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng hiện đang bị khai thác trong thực tế.</p> <p>- Ảnh hưởng: <b>Máy tính</b> cài đặt Windows 10.</p>	<a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43491">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43491</a>
2	CVE-2024-38018 CVE-2024-38227 CVE-2024-38228 CVE-2024-43464	<p>- Điểm CVSS: 8.8 (Nghiêm trọng)- Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.</p> <p>- Ảnh hưởng: <b>Hệ thống</b> cài đặt Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server Subscription Edition.</p>	<a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-38018">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-38018</a> <a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-38227">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-38227</a> <a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-38228">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-38228</a> <a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43464">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43464</a>
3	CVE-2024-43461	<p>- Điểm CVSS: 8.8 (Cao)- Mô tả: Lỗ hổng trong Windows MSHTML Platform cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing).</p> <p>- Ảnh hưởng: <b>Máy tính</b> cài đặt Windows 10, Windows 11, <b>Hệ</b></p>	<a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43461">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43461</a>

		<b>thông</b> cài đặt Windows Server 2008, 2012, 2016, 2019, 2022.	
4	CVE-2024-21416 CVE-2024-38045	- Điểm CVSS: 8.1 (Cao)- Mô tả: Lỗ hổng trong Windows TCP/IP cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, <b>Hệ thống</b> cài đặt Windows Server 2019, 2022.	<a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-21416">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-21416</a> <a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-38045">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-38045</a>
5	CVE-2024-38014	- Điểm CVSS: 7.8 (Cao)- Mô tả: Lỗ hổng trong Windows Installer cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: <b>Máy tính</b> cài đặt Windows 10, Windows 11, <b>Hệ thống</b> cài đặt Windows Server 2008, 2012, 2016, 2019, 2022.	<a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-38014">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-38014</a>
6	CVE-2024-43463	- Điểm CVSS: 7.8 (Cao)- Mô tả: Lỗ hổng trong Microsoft Office Visio cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: <b>Máy tính</b> cài đặt Microsoft Visio 2016, Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise, Microsoft Office 2019.	<a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43463">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43463</a>
7	CVE-2024-38226	- Điểm CVSS: 7.3 (Cao)- Mô tả: Lỗ hổng trong Microsoft Publisher cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong	<a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-38226">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-38226</a>

		<p>thực tế.</p> <p>- Ảnh hưởng: <b>Máy tính</b> cài đặt Microsoft Publisher 2016, Microsoft Office LTSC 2021, Microsoft Office 2019.</p>	
8	<p>CVE-2024-38217</p> <p>CVE-2024-43487</p>	<p>- Điểm CVSS: 5.4 (Cao)- Mô tả: Lỗ hổng trong Windows Mark of the Web cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế.</p> <p>- Ảnh hưởng: <b>Máy tính</b> cài đặt Windows 10, Windows 11, <b>Hệ thống</b> cài đặt Windows Server 2008, 2012, 2016, 2019, 2022.</p>	<p><a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-38217">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-38217</a></p> <p><a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43487">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43487</a></p>
9	<p>CVE-2024-43468</p>	<p>- Điểm CVSS: 9.8 (Nghiêm trọng)- Mô tả: Lỗ hổng trong Microsoft Configuration Manager cho phép đối tượng tấn công thực thi mã từ xa.</p> <p>- Ảnh hưởng: <b>Hệ thống/Máy tính</b> cài đặt Microsoft Configuration Manager.</p>	<p><a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43468">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43468</a></p>
10	<p>CVE-2024-43582</p>	<p>- Điểm CVSS: 8.1 (Nghiêm trọng)- Mô tả: Lỗ hổng trong Remote Desktop Protocol Server cho phép đối tượng tấn công thực thi mã từ xa.</p> <p>- Ảnh hưởng: <b>Máy tính</b> cài đặt Windows 10, Windows 11, <b>Hệ thống</b> cài đặt Windows Server 2019, 2022.</p>	<p><a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43582">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43582</a></p>
11	<p>CVE-2024-43572</p>	<p>- Điểm CVSS: 7.8 (Cao)- Mô tả: Lỗ hổng trong Microsoft</p>	<p><a href="https://msrc.microsoft.com/updateguide/vulnerability/CV">https://msrc.microsoft.com/updateguide/vulnerability/CV</a></p>

		<p>Management Console cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng hiện đang bị khai thác trong thực tế.</p> <p>- Ảnh hưởng: <b>Máy tính</b> cài đặt Windows 10, Windows 11, <b>Hệ thống</b> cài đặt Windows Server 2008, 2012, 2016, 2019, 2022.</p>	E-2024-43572
12	CVE-2024-43583	<p>- Điểm CVSS: 7.8 (Cao)- Mô tả: Lỗ hổng trong Microsoft Winlogon cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Thông tin chi tiết về lỗ hổng đã được công bố công khai.</p> <p>- Ảnh hưởng: <b>Máy tính</b> cài đặt Windows 10, Windows 11, <b>Hệ thống</b> cài đặt Windows Server 2008, 2012, 2016, 2019, 2022.</p>	<p><a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43583">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43583</a></p>
13	CVE-2024-43504	<p>- Điểm CVSS: 7.8 (Cao)- Mô tả: Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.</p> <p>- Ảnh hưởng: <b>Máy tính</b> cài đặt Microsoft Excel 2016, 2019. Microsoft Office LTSC 2021, 2024. Microsoft 365 Apps for Enterprise.</p>	<p><a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43504">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43504</a></p>
14	<p>CVE-2024-43576</p> <p>CVE-2024-43616</p>	<p>- Điểm CVSS: 7.8 (Cao)- Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.</p> <p>- Ảnh hưởng: <b>Máy tính</b> cài đặt Microsoft Office LTSC 2024. Microsoft 365 Apps for</p>	<p><a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43576">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43576</a></p> <p><a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43616">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43616</a></p>

		Enterprise.	
15	CVE-2024-43505	<p>- Điểm CVSS: 7.8 (Cao)- Mô tả: Lỗ hổng trong Microsoft Office Visio cho phép đối tượng tấn công thực thi mã từ xa.</p> <p>- Ảnh hưởng: <b>Máy tính</b> cài đặt Microsoft Office LTSC 2021, 2024. Microsoft 365 Apps for Enterprise, Microsoft Office 2019.</p>	<p><a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43505">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43505</a></p>
16	CVE-2024-43573	<p>- Điểm CVSS: 6.5 (Trung bình)- Mô tả: Lỗ hổng trong Windows MSHTML Platform cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). Lỗ hổng hiện đang bị khai thác trong thực tế.</p> <p>- Ảnh hưởng: <b>Máy tính</b> cài đặt Windows 10, Windows 11, <b>Hệ thống</b> cài đặt Windows Server 2012, 2016, 2019, 2022.</p>	<p><a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43573">https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-43573</a></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/2024/10/8/the-october-2024-security-update-review>

**DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN**  
(Kèm theo Công văn số /TTCNTT-HTATTT ngày /10/2024  
của Trung tâm Công nghệ thông tin)

<b>TT</b>	<b>Tên đơn vị</b>
1.	Thanh tra Bộ
2.	Cục Phát triển công nghệ và Đổi mới sáng tạo.
3.	Cục Thông tin khoa học và công nghệ quốc gia
4.	Cục Phát triển thị trường và doanh nghiệp khoa học và công nghệ
5.	Cục An toàn bức xạ và hạt nhân
6.	Cục Sở hữu trí tuệ
7.	Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia
8.	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
9.	Viện Khoa học và công nghệ Việt Nam - Hàn Quốc (VKIST)
10.	Viện Nghiên cứu sáng chế và Khai thác công nghệ
11.	Viện Năng lượng nguyên tử Việt Nam
12.	Viện Ứng dụng công nghệ
13.	Viện Đánh giá khoa học và Định giá công nghệ
14.	Viện Khoa học sở hữu trí tuệ
15.	Viện Nghiên cứu và Phát triển Vùng
16.	Văn phòng các Chương trình trọng điểm cấp nhà nước
17.	Văn phòng Công nhận chất lượng
18.	Văn phòng Đăng ký hoạt động khoa học và công nghệ
19.	Văn phòng các Chương trình khoa học và công nghệ quốc gia
20.	Báo VnExpress
21.	Tạp chí Khoa học và Công nghệ Việt Nam
22.	Nhà xuất bản Khoa học và Kỹ thuật
23.	Quỹ Phát triển khoa học và công nghệ quốc gia
24.	Quỹ Đổi mới công nghệ quốc gia
25.	Trung tâm Nghiên cứu và Phát triển truyền thông khoa học và công nghệ
26.	Trung tâm Nghiên cứu và Phát triển hội nhập khoa học và công nghệ quốc tế
27.	Trung tâm Công nghệ thông tin