

Số: /TTCNTT-HTATTT
V/v lỗ hổng an toàn thông tin ảnh hưởng
cao và nghiêm trọng trong các sản phẩm
Microsoft công bố tháng 12/2024

Hà Nội, ngày tháng 12 năm 2024

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

Ngày 10/12/2024, Microsoft đã phát hành danh sách bản vá tháng 12/2024 với **72 lỗ hổng an toàn thông tin** gồm có **71 lỗ hổng an toàn thông tin** trong các sản phẩm của hãng Microsoft và **01 lỗ hổng an toàn thông tin** trong các sản phẩm thuộc bên thứ ba có ảnh hưởng tới Microsoft, Trong đó có 06 lỗ hổng mức Nghiêm trọng và 54 lỗ hổng mức độ Cao:

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 đơn vị.

Lỗ hổng an toàn thông tin tồn tại trên một số sản phẩm của Microsoft như: Windows và các thành phần của Windows, Office và các thành phần của Office, SharePoint Server, Hyper-V, Defender cho Endpoint, System Center Operations Manager.

Thông tin chi tiết về lỗ hổng an toàn thông tin tại Phụ lục kèm theo

Trung tâm Công nghệ thông tin đề nghị Quý đơn vị cứu thông tin về các lỗ hổng an toàn thông tin nêu trên, thực hiện rà soát hệ thống, xử lý các vấn đề về an toàn thông tin mạng trên hệ thống thuộc phạm vi quản lý và gửi kết quả báo cáo rà soát về địa chỉ thư điện tử **phongktht@most.gov.vn** **chậm nhất trước ngày 28 hàng tháng**.

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 / 12 /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-2024-49138	<ul style="list-style-type: none">- Điểm CVSS: 7.8 (Cao)- Mô tả: Lỗ hổng trong Windows Common Log File System Driver cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.- Ảnh hưởng: Máy tính cài đặt Windows 10, Windows 11; Hệ thống cài đặt Windows Server 2008, 2012, 2016, 2019, 2022, 2025.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-49138
2	CVE-2024-49112 CVE-2024-49127	<ul style="list-style-type: none">- Điểm CVSS: 9.8 (Nghiêm trọng)- Mô tả: Lỗ hổng trong Windows Lightweight Directory Access Protocol (LDAP) cho phép đối tượng tấn công thực thi mã từ xa.- Ảnh hưởng: Máy tính cài đặt Windows 10, Windows 11; Hệ thống cài đặt Windows Server 2008, 2012, 2016, 2019, 2022, 2025.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-49112 https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-49127

3	CVE-2024-49117	<ul style="list-style-type: none"> - Điểm CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Máy tính cài đặt Windows 10, Windows 11; Hệ thống cài đặt Windows Server 2022, 2025. 	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-49117
4	CVE-2024-49124	<ul style="list-style-type: none"> - Điểm CVSS: 8.1 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Lightweight Directory Access Protocol (LDAP) Client cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Máy tính cài đặt Windows 10, Windows 11; Hệ thống cài đặt Windows Server 2008, 2012, 2016, 2019, 2022, 2025. 	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-49124
5	CVE-2024-49126	<ul style="list-style-type: none"> - Điểm CVSS: 8.1 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Local Security Authority Subsystem Service (LSASS) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Máy tính cài đặt Windows 10, Windows 11; Hệ thống cài đặt Windows Server 2008, 2012, 2016, 2019, 2022, 2025. 	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-49126

6	CVE-2024-49070	<p>- Điểm CVSS: 7.4 (Cao)</p> <p>- Mô tả: Lỗ hổng trong Microsoft SharePoint cho phép đối tượng tấn công thực thi mã từ xa.</p> <p>- Ảnh hưởng: Hệ thống cài đặt Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016.</p>	<p>https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-49070</p>
7	CVE-2024-49068	<p>- Điểm CVSS: 8.2 (Cao)</p> <p>- Mô tả: Lỗ hổng trong Microsoft SharePoint cho phép đối tượng tấn công thực hiện leo thang đặc quyền.</p> <p>- Ảnh hưởng: Hệ thống cài đặt Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016</p>	<p>https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-49068</p>
8	CVE-2024-49142	<p>- Điểm CVSS: 7.8 (Cao)</p> <p>- Mô tả: Lỗ hổng trong Microsoft Access cho phép đối tượng tấn công thực thi mã từ xa.</p> <p>- Ảnh hưởng: Máy tính cài đặt Microsoft Access 2016, Microsoft Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise, Microsoft Office</p>	<p>https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-49142</p>

		2019.	
9	CVE-2024-49069	<p>- Điểm CVSS: 7.8 (Cao)</p> <p>- Mô tả: Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.</p> <p>- Ảnh hưởng: Máy tính cài đặt Microsoft Excel 2016, Microsoft Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise, Microsoft Office 2019.</p>	<p>https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-49069</p>
10	CVE-2024-49065	<p>- Điểm CVSS: 5.5 (Cao)</p> <p>- Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.</p> <p>- Ảnh hưởng: Máy tính cài đặt Microsoft Word 2016, Microsoft Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise, Microsoft Office 2019; Hệ thống cài đặt Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016.</p>	<p>https://msrc.microsoft.com/updateguide/vulnerability/CVE-2024-49065</p>

2. Khuyến nghị giải pháp

Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng;

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;

Kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows có khả

năng bị ảnh hưởng. 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 sau:

<https://msrc.microsoft.com/update-guide/>

<https://www.zerodayinitiative.com/blog/2024/12/10/the-december-2024-security-update-review>

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN
(Kèm theo Công văn số /TTCNTT-HTATTT ngày /12/2024
của Trung tâm Công nghệ thông tin)

TT	Tên đơn vị
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