

BỘ TƯ PHÁP
CỤC CÔNG NGHỆ THÔNG TIN

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

Số: /CNTT-HT&ATTT
V/v Cảnh báo lỗ hổng bảo mật ảnh hưởng
cao trong các sản phẩm Microsoft công bố
tháng 05/2024.

Hà Nội, ngày tháng 05 năm 2024

- Kính gửi:
- Thủ trưởng các đơn vị thuộc Bộ;
 - Giám đốc Sở Tư pháp các tỉnh, thành phố trực thuộc Trung ương;
 - Cục trưởng Cục Thi hành án dân sự các tỉnh, thành phố trực thuộc Trung ương.

Hiện nay, tình hình an toàn an ninh thông tin mạng trong nước và quốc tế đang có diễn biến phức tạp, các đơn vị chuyên trách về an toàn an ninh thông tin mạng liên tục đưa ra các cảnh báo, khuyến nghị về công tác đảm bảo an toàn an ninh thông tin mạng. Ngày 14/05/2024, Microsoft đã phát hành danh sách các bản vá tháng 05/2024 với 59 lỗ hổng bảo mật trong các sản phẩm của mình. Tin tặc lợi dụng các lỗ hổng bảo mật này nhằm tấn công thực thi mã từ xa; tấn công vượt qua cơ chế bảo vệ; tấn công giả mạo; tấn công leo thang đặc quyền; tấn công XXE.

Nhằm bảo đảm an toàn, an ninh thông tin mạng và phòng tránh nguy cơ bị tấn công vào hệ thống mạng của đơn vị, Cục Công nghệ thông tin đề nghị Quý đơn vị Kiểm tra, rà soát và xác định máy chủ, máy trạm sử dụng hệ điều hành Windows và các sản phẩm của Microsoft có khả năng bị ảnh hưởng; Thực hiện cập nhật bản vá bảo mật theo khuyến cáo của Microsoft (*Chi tiết tại Phụ lục kèm theo công văn này*).

Trong quá trình thực hiện nếu có khó khăn, vướng mắc, đề nghị Quý đơn vị phản ánh kịp thời về Cục Công nghệ thông tin để được hướng dẫn, hỗ trợ.

Thông tin đầu mối liên hệ:

- Họ và tên: Trần Văn Dũng
- Chức vụ: Chuyên viên Phòng Hạ tầng và an toàn thông tin
- Số điện thoại: 024.62739717
- Địa chỉ thư điện tử: tranvandung@moj.gov.vn

Cục Công nghệ thông tin trân trọng cảm ơn sự quan tâm, phối hợp của Quý đơn vị./.

Nơi nhận:

- Như trên;
- Thứ trưởng Mai Lương Khôi (để b/c);
- Cục trưởng (để b/c);
- Lưu: VT, HT&ATTT.

**KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG**

Tạ Thành Trung

PHỤ LỤC: HƯỚNG DẪN CHI TIẾT LỖ HỔNG BẢO MẬT TRONG CÁC SẢN PHẨM MICROSOFT

1. Thông tin các lỗ hổng an toàn thông tin

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-30040	<ul style="list-style-type: none">- Điểm: CVSS: 8.8 (Cao)- Mô tả: Lỗ hổng trong Windows MSHTML Platform cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế.- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30040
2	CVE-2024-30044	<ul style="list-style-type: none">- 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.- Ảnh hưởng: Microsoft SharePoint Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30044
3	CVE-2024-30051 CVE-2024-30032 CVE-2024-30035	<ul style="list-style-type: none">- Điểm: CVSS: 7.8 (Cao)- Mô tả: Lỗ hổng trong Windows DWM Core Library cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30051 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30032 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30035

4	CVE-2024-30042	<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 Online Server, Microsoft 365 Apps, Microsoft Office LTSC. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30042
5	CVE-2024-30033	<ul style="list-style-type: none"> - Điểm: CVSS: 7.0 (Cao) - Mô tả: Lỗ hổng trong Windows Search Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30033
6	CVE-2024-30043	<ul style="list-style-type: none"> - Điểm: CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện tấn công XXE. - Ảnh hưởng: Microsoft SharePoint Server. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30043

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/2024/5/14/the-may-2024-security-update-review>