BỘ TƯ PHÁP
CỤC CÔNG NGHỆ THÔNG TIN

Số:943 /CNTT-HT&ATTT
V/v Cảnh báo lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 12/2023.

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

Hà Nội, ngày 25 tháng 12 năm 2023

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 12/12/2023, Microsoft đã phát hành danh sách các bản vá tháng 12/2023 với 33 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 thực hiện nâng cao đặc quyền.

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

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN
BỘ TƯ PHÁP

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-2023-36019	- Điểm: CVSS: 9.6 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Power Platform Connector cho phép đối tượng tấn công thực hiện tấn công giả mạo, dẫn tới thực thi mã từ xa ở phía người dùng. - Ảnh hưởng: Microsoft Power Platform, Azure Logic Apps.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36019
2	CVE-2023-35630 CVE-2023-35641	- Điểm: CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Internet Connection Sharing (ICS) 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-2023-35630 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35641
3	CVE-2023-35628	- Điểm: CVSS: 8.1 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows MSHTML Platform cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35628

STT	CVE	Mô tả	Link tham khảo
		- Ảnh hưởng: Windows 10, Windows 11; Windows Server 2008, 2012, 2016, 2019, 2022.	
4	CVE-2023-35636	- Điểm: CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng trong Microsoft Outlook làm lộ lọt NTML hash, cho phép đối tượng tấn công thực hiện leo thang đặc quyền. - Ảnh hưởng: Microsoft Office 2016, 2019; Microsoft Office LTSC 2021; Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35636

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/2023/12/12/the-december-2023-security-update-review