BỘ TƯ PHÁP
CỤC CÔNG NGHỆ THÔNG TIN

Số: 344 /CNTT-HT&ATTT
V/v Cảnh báo lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 04/2024.

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

Hà Nội, ngày 22 tháng 04 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 09/04/2024, Microsoft đã phát hành danh sách các bản vá tháng 04/2024 với 147 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.

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 XHCN VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN
BỘ TƯ PHÁP

Tạ Thanh 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-2024-20678	- 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	- 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	- 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. - Ảnh hưởng: Microsoft Defender for IoT.	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

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	CVE-2024-26221 CVE-2024-26222 CVE-2024-26223 CVE-2024-26224 CVE-2024-26227 CVE-2024-26231 CVE-2024-26233	- 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.	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
8	CVE-2024-26234	- 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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26234

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