

BỘ NÔNG NGHIỆP
VÀ PHÁT TRIỂN NÔNG THÔN
TRUNG TÂM CHUYÊN ĐỔI SỐ
VÀ THỐNG KÊ NÔNG NGHIỆP

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

Số: /CDS
V/v lỗ hổng an toàn thông tin ảnh hưởng
cao và nghiêm trọng trong các sản phẩm
Microsoft công bố tháng 06/2024

Hà Nội, ngày tháng năm 2024

Kính gửi: Các đơn vị trực thuộc Bộ

Ngày 14/06/2024, Trung tâm Chuyên đổi số và Thống kê nông nghiệp nhận được văn bản số 1096/CATTT-NCSC của Cục An toàn thông tin – Bộ Thông tin và Truyền thông thông báo ngày 11/06/2024, hãng Microsoft đã phát hành danh sách bản vá tháng 06 với 49 lỗ hổng an toàn thông tin trong các sản phẩm của mình. 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:

- Lỗ hổng an toàn thông tin **CVE-2024-30080** trong Microsoft Message Queuing (MSMQ) cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-30103** trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-30078** trong Windows Wi-Fi Driver cho phép đối tượng tấn công thực thi mã từ xa.

- 03 lỗ hổng an toàn thông tin **CVE-2024-30101, CVE-2024-30102, CVE-2024-30104** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-30100** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

(Thông tin chi tiết các lỗ hổng bảo mật có tại Phụ lục kèm theo)

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của cơ quan, đơn vị thuộc Bộ, Trung tâm Chuyên đổi số và Thống kê nông nghiệp khuyến nghị Quý đơn vị thực hiện một số biện pháp chính như sau:

1. Kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows 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.

3. Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ: Trung tâm Chuyển đổi số và Thống kê nông nghiệp, điện thoại: 02437341635 (máy lẻ: 308), Email: quantrimang@mard.gov.vn hoặc Trung tâm Giám sát an toàn không gian mạng quốc gia – Cục An toàn thông tin, điện thoại 02432091616, Email: ncsc@ais.gov.vn.

Trân trọng./.

Nơi nhận:

- Như trên;
- Thứ trưởng Nguyễn Hoàng Hiệp (để b/c);
- Ban Giám đốc (để b/c);
- Lưu: VT, QTHT.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Nguyễn Kim Phúc

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG AN TOÀN THÔNG TIN
TRONG SẢN PHẨM MICROSOFT

(Kèm theo Công văn số /CĐS
 ngày / /2024 của Trung tâm Chuyển đổi số và Thống kê nông nghiệp)

1. Thông tin các lỗ hổng an toàn thông tin

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-30080	<ul style="list-style-type: none"> - Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Message Queuing (MSMQ) 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-2024-30080
2	CVE-2024-30103	<ul style="list-style-type: none"> - Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Outlook 2016, 2019, Microsoft 365 Apps for Enterprise, Microsoft Office LTSC 2021. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30103
3	CVE-2024-30078	<ul style="list-style-type: none"> - Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Windows Wi-Fi Driver 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-2024-30078

4	CVE-2024-30101 CVE-2024-30102 CVE-2024-30104	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Outlook 2016, 2019, Microsoft 365 Apps for Enterprise, Microsoft Office LTSC 2021. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30101 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30102 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30104
5	CVE-2024-30100	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server Subscription Edition. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30100

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/2024/6/11/the-june-2024-security-update-review>.