

**ỦY BAN NHÂN DÂN
HUYỆN VĂN LÂM**

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

Số: /UBND-VHTT
V/v lỗ hổng an toàn thông tin
ảnh hưởng cao và nghiêm trọng
trong các sản phẩm Microsoft
công bố tháng 7/2024

Văn Lâm, ngày tháng 7 năm 2024

Kính gửi:

- Các phòng, ban, ngành, đoàn thể huyện;
- UBND các xã, thị trấn.

Theo thông báo của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft, với 139 lỗ hổng an toàn thông tin trong các sản phẩm của Microsoft. Trong đó đáng chú ý các lỗ hổng bảo mật sau:

- 03 lỗ hổng an toàn thông tin **CVE-2024-38074, CVE-2024-38076, CVE-2024-38077** trong Windows Remote Desktop Licensing Service cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-38060** trong Windows Imaging Component cho phép đối tượng tấn công thực thi mã từ xa.

- 03 lỗ hổng an toàn thông tin **CVE-2024-38023, CVE-2024-38024, CVE-2024-38094** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-38021** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-38080** trong Windows Hyper-V cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2024-38112** trong Windows MSHTML Platform cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). Lỗ hổng hiện đang bị khai thác trong thực tế.

Thực hiện Công văn số 949/STTTT-BCVTCNTT ngày 15/7/2024 của Sở Thông tin và Truyền thông tỉnh Hưng Yên về lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 7/2024. Để đảm bảo an toàn hệ thống thông tin dùng chung của huyện và của các cơ quan, đơn vị trên địa bàn; Ủy ban nhân dân huyện Văn Lâm yêu cầu Thủ trưởng các cơ quan, đơn vị, địa phương chỉ đạo các bộ phận chuyên môn triển khai thực hiện rà soát, khắc phục các lỗ hổng bảo mật trên theo các khuyến nghị sau:

1. Thực hiện Kiểm tra, rà soát, xác định máy 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 đính kèm*)

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 cần hỗ trợ cơ quan, đơn vị liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại 02432091616, thư điện tử: ais@mic.gov.vn./.

Nơi nhận:

- Như trên;
- Lãnh đạo UBND huyện;
- Lưu VT.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Hoàng Thế Vĩnh

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

(Kèm theo Công văn số /UBND-VHTT ngày /7/2024
của UBND huyện Văn Lâm)

1. Thông tin về các lỗ hổng an toàn thông tin

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-38074 CVE-2024-38076 CVE-2024-38077	<ul style="list-style-type: none"> - Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Remote Desktop Licensing Service cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008, 2012, 2016, 2019, 2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38074 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38076 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38077
2	CVE-2024-38060	<ul style="list-style-type: none"> - Điểm CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Imaging Component 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-2024-38060
3	CVE-2024-38023 CVE-2024-38024 CVE-2024-38094	<ul style="list-style-type: none"> - Điểm CVSS: 7.2 (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 2019, Microsoft SharePoint 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38023 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38024 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38094

		Enterprise Server 2016, Microsoft SharePoint Server Subscription Edition.	com/update-guide/vulnerability/CVE-2024-38094
4	CVE-2024-38021	<ul style="list-style-type: none"> - Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office 2016, 2019, Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38021
5	CVE-2024-38080	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 11, Windows Server 2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38080
6	CVE-2024-38112	<ul style="list-style-type: none"> - Điểm CVSS: 7.5 (Cao) - Mô tả: Lỗ hổng trong Windows MSHTML Platform cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112

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/2024/7/9/the-july-2024-security-update-review>