UBND HUYỆN EA SÚP
**PHÒNG VĂN HOÁ VÀ THÔNG TIN**

Số: 312 /PVHTT
V/v hướng dẫn khắc phục lỗ hổng bảo mật ảnh hưởng mức cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 7/2024

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

*Ea Súp, ngày 23 tháng 7 năm 2024*

Kính gửi:

- Các cơ quan, đơn vị trên địa bàn huyện;
- UBND các xã, Thị trấn.

Ngày 09/7/2024, Microsoft đã phát hành danh sách bản vá tháng 7/2024 với **139 lỗ hổng bảo mật** trong các sản phẩm của mình. Bản phát hành tháng này, đặc biệt đáng chú ý; các lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng *(Có Phụ lục gửi kèm theo)*.

Thực hiện Công văn số 1341/STTTT-CNTT ngày 15/07/2024 của Sở Thông tin truyền thông về việc hướng dẫn khắc phục lỗ hổng bảo mật ảnh hưởng mức cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 7/2024. Đồng thời, nhằm đảm bảo an toàn thông tin cho các hệ thống thông tin của cơ quan, đơn vị trên địa bàn tỉnh. Phòng Văn hoá và Thông tin huyện Ea Súp khuyến nghị các cơ quan, đơn vị, UBND các xã, thị trấn triển khai các nội dung 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 về lỗ hổng bảo mật tại Phụ lục gửi 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 được hỗ trợ, các cơ quan, đơn vị liên hệ đầu mối hỗ trợ của Cục An toàn thông tin và Sở Thông tin và Truyền thông:

**- Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại: 0243.2091.616, thư điện tử: ncsc@ais.gov.vn.**

**- Trung tâm Giám sát, điều hành đô thị thông minh: Đồng chí Lê Xuân Quang, Phó Giám đốc Trung tâm, điện thoại 0975.001.578; thư điện tử: quanglx@tttt.daklak.gov.vn.**

Nhận được Công văn này, đề nghị các cơ quan, đơn vị, UBND các xã; thị trấn quan tâm, triển khai thực hiện./.

***Nơi nhận:***
- Như trên;
- Sở Thông tin và Truyền thông; } Thay b/c
- UBND huyện Ea Súp;
- Lưu: VT, VHTT.

**TRƯỞNG PHÒNG**

PHÒNG VĂN HÓA VÀ THÔNG TIN

**Phương Khánh Giang**

**PHỤ LỤC**

**Thông tin về các lỗ hổng an toàn thông tin trong các sản phẩm Microsoft**

*(Kèm theo Công văn số: /PVHTT ngày / 7 /2024 của Phòng Văn hoá và Thông tin)*

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

| STT | CVE | Mô tả | Link tham khảo |
|---|---|---|---|
| 1 | CVE-2024-38074<br>CVE-2024-38076<br>CVE-2024-38077 | - Điểm CVSS: 9.8 (Nghiêm trọng)<br>- Mô tả: Lỗ hổng trong Windows Remote Desktop Licensing Service cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Windows Server 2008, 2012, 2016, 2019, 2022. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38074<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38076<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38077 |
| 2 | CVE-2024-38060 | - Điểm CVSS: 8.8 (Nghiêm trọng)<br>- Mô tả: Lỗ hổng trong Windows Imaging Component cho phép đối tượng tấn công thực thi mã từ xa.<br>- 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<br>CVE-2024-38024<br>CVE-2024-38094 | - Điểm CVSS: 7.2 (Nghiêm trọng)<br>- Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38023<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38024<br>https://msrc.microsoft.com/update- |

| | | | |
|---|---|---|---|
| | | Microsoft SharePoint Server Subscription Edition. | guide/vulnerability/CVE-2024-38094 |
| 4 | CVE-2024-38021 | - Điểm CVSS: 8.8 (Cao)<br>- Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.<br>- 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 | - Điểm CVSS: 7.8 (Cao)<br>- 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.<br>- Ảnh hưởng: Windows 11, Windows Server 2022. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38080 |
| 6 | CVE-2024-38112 | - Điểm CVSS: 7.5 (Cao)<br>- 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.<br>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112 |

| **STT** | **CVE** | **Mô tả** | **Link tham khảo** |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1 | CVE-2024-30080 | - Điểm CVSS: 9.8 (Nghiêm trọng)<br>- Mô tả: Lỗ hổng trong Microsoft Message Queuing (MSMQ) cho phép đối tượng tấn công thực thi mã từ xa.<br>- 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 | - Điểm CVSS: 8.8 (Cao)<br>- Mô tả: Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa.<br>- 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 | - Điểm CVSS: 8.8 (Cao)<br>- Mô tả: Lỗ hổng trong Windows Wi-Fi Driver cho phép đối tượng tấn công thực thi mã từ xa.<br>- 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<br>CVE-2024-30102<br>CVE-2024-30104 | - Điểm CVSS: 7.8 (Cao)<br>- Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.<br>- 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<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30102<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30104 |

| | | | |
|---|---|---|---|
| 5 | CVE-2024-30100 | - Điểm CVSS: 7.8 (Cao)<br>- Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.<br>- 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/2024/7/9/the-july-2024-security-update-review