

UBND TỈNH ĐẮK LẮK  
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: /STTTT-CNTT  
V/v lỗ hổng an toàn thông tin ảnh  
hưởng cao và nghiêm trọng trong các  
sản phẩm Microsoft công bố tháng  
08/2024

Đắk Lắk, ngày tháng năm 2024

Kính gửi:

- Các sở, ban, ngành của tỉnh;
- UBND các huyện, thị xã, thành phố.

Theo khuyến nghị của Cục An toàn thông tin, Bộ Thông tin và Truyền thông tại Công văn 1667/CATTT-NCSC ngày 19/8/2024 (Có văn bản kèm theo), Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị triển khai các nội dung về đảm bảo an toàn thông tin, cụ thể:

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 (thông tin chi tiết về các lỗ hổng an toàn thông tin và cách khắc phục tham khảo 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 các 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 của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại: 02432091616, thư điện tử: ncsc@ais.gov.vn.

Sở Thông tin và Truyền thông kính đề nghị các cơ quan, đơn vị quan tâm, triển khai các nội dung như trên./.

**Nơi nhận:**

- Như trên;
- UBND tỉnh (b/c);
- Cục An toàn thông tin (b/c);
- ĐAKLAKIOC (t/h);
- Lưu: VT, CNTT.

**GIÁM ĐỐC**

**Trương Hoài Anh**

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

(Kèm theo Công văn số /STTTT-CNTT ngày tháng 08/2024 của Sở Thông tin và Truyền thông)

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

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-38063	<ul style="list-style-type: none"> <li>- Điểm CVSS: 9.8 (Nghiêm trọng)</li> <li>- Mô tả: Lỗ hổng trong Windows TCP/IP cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063</a>
2	CVE-2024-38199	<ul style="list-style-type: none"> <li>- Điểm CVSS: 9.8 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Windows Line Printer Daemon (LPD) Service cho phép đối tượng tấn công thực thi mã từ xa. Thông tin chi tiết về lỗ hổng đã được công bố công khai.</li> <li>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199</a>
3	CVE-2024-38189	<ul style="list-style-type: none"> <li>- Điểm CVSS: 8.8 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Microsoft Project cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng hiện đang bị khai</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38189">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38189</a>

		<p>thác trong thực tế.</p> <ul style="list-style-type: none"> <li>- Ảnh hưởng: Microsoft Project 2016, Microsoft Office 2019, Microsoft 365 Apps for Enterprise, Microsoft Office LTSC 2021.</li> </ul>	
4	<p>CVE-2024-38218</p> <p>CVE-2024-38219</p>	<ul style="list-style-type: none"> <li>- Điểm CVSS: 8.4 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Microsoft Edge cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Microsoft Edge (Chromium-based).</li> </ul>	<p><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38218">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38218</a></p> <p><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38219">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38219</a></p>
5	CVE-2024-38193	<ul style="list-style-type: none"> <li>- Điểm CVSS: 7.8 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Windows Ancillary Function Driver for WinSock cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.</li> <li>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.</li> </ul>	<p><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193</a></p>
6	CVE-2024-38107	<ul style="list-style-type: none"> <li>- Điểm CVSS: 7.8 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Windows Power Dependency Coordinator cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.</li> </ul>	<p><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107</a></p>

		- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022.	
7	CVE-2024-38170 CVE-2024-38172	<ul style="list-style-type: none"> <li>- Điểm CVSS: 7.8 (Cao)</li> <li>- Mô tả: Lỗi hỏng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Microsoft 365 Apps for Enterprise, Microsoft Office LTSC for Mac 2021.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38170">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38170</a>  <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38172">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38172</a>
8	CVE-2024-38171	<ul style="list-style-type: none"> <li>- Điểm CVSS: 7.8 (Cao)</li> <li>- Mô tả: Lỗi hỏng trong Microsoft PowerPoint cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Microsoft PowerPoint 2016, Microsoft Office 2019, Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38171">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38171</a>
9	CVE-2024-38178	<ul style="list-style-type: none"> <li>- Điểm CVSS: 7.5 (Cao)</li> <li>- Mô tả: Lỗi hỏng trong Scripting Engine cho phép đối tượng tấn công thực thi mã từ xa. Lỗi hỏng hiện đang bị khai thác trong thực tế.</li> <li>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178</a>

10	CVE-2024-38202	<ul style="list-style-type: none"> <li>- Điểm CVSS: 7.3 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Windows Update Stack cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Thông tin chi tiết về lỗ hổng đã được công bố công khai.</li> <li>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38202">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38202</a>
11	CVE-2024-38106	<ul style="list-style-type: none"> <li>- Điểm CVSS: 7.0 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Windows Kernel cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.</li> <li>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106</a>
12	CVE-2024-21302	<ul style="list-style-type: none"> <li>- Điểm CVSS: 6.7 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Windows Secure Kernel Mode cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Thông tin chi tiết về lỗ hổng đã được công bố công khai.</li> <li>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21302">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21302</a>

13	CVE-2024-38173	<ul style="list-style-type: none"> <li>- Điểm CVSS: 6.7 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Microsoft Outlook 2016, Microsoft Office 2019, Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38173">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38173</a>
14	CVE-2024-38200	<ul style="list-style-type: none"> <li>- Điểm CVSS: 6.5 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). Thông tin chi tiết về lỗ hổng đã được công bố công khai.</li> <li>- Ảnh hưởng: Microsoft Office 2016, 2019, Microsoft 365 Apps for Enterprise, Microsoft Office LTSC 2021.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38200">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38200</a>
15	CVE-2024-38213	<ul style="list-style-type: none"> <li>- Điểm CVSS: 6.5 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Windows Mark of the Web Security cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế.</li> <li>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213</a>

## 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/2024/8/13/the-august-2024-security-update-review>