

Số: /STTTT-CNTT&BCVT  
V/v lỗ hổng bảo mật ảnh hưởng cao  
và nghiêm trọng trong các sản phẩm Microsoft  
công bố tháng 12/2022

Tuyên Quang, ngày tháng 12 năm 2022

Kính gửi:

- Văn phòng Đoàn Đại biểu Quốc hội và Hội đồng nhân dân;
- Văn phòng Ủy ban nhân dân tỉnh;
- Các sở, ban, ngành;
- Ủy ban nhân dân các huyện, thành phố.

Căn cứ văn bản số 2035/CATTT–NCSC ngày 14/12/2022 của Cục An toàn thông tin về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2022, Sở Thông tin và Truyền thông cung cấp thông tin và đưa ra các giải pháp phòng, tránh khai thác lỗ hổng bảo mật cao và nghiêm trọng trong các sản phẩm Microsoft như sau:

### **I. Thông tin về lỗ hổng bảo mật trong các sản phẩm Microsoft**

Ngày 13/12/2022, Microsoft đã phát hành danh sách bản vá tháng 12 với 52 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 sau:

- Lỗ hổng bảo mật **CVE-2022-44698** trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật. Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật **CVE-2022-41076** trong PowerShell cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này ảnh hưởng đến nhiều sản phẩm như: Microsoft Exchange Server, Skype for Business Server,...

- Lỗ hổng bảo mật **CVE-2022-44713** trong Microsoft Outlook for Mac cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing).

- Lỗ hổng bảo mật **CVE-2022-44699** trong Azure Network Watcher Agent cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật.

- Lỗ hổng **CVE-2022-44710** trong DirectX Graphics Kernel cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã có mã khai thác được công bố rộng rãi trên Internet.

- 02 lỗ hổng bảo mật **CVE-2022-44690, CVE-2022-44693** trong Microsoft

SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- 02 lỗ hổng bảo mật **CVE-2022-44678, CVE-2022-44681** trong Windows Print Spooler cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

- 02 lỗ hổng bảo mật **CVE-2022-44708, CVE-2022-41115** trong Microsoft Edge (Chromium-based) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-44673** trong Windows Client Server Run-Time Subsystem (CSRSS) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

*Thông tin chi tiết các lỗ hổng bảo mật có tại phụ lục kèm theo.*

## **II. Các giải pháp phòng tránh**

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông Khuyến nghị Quý đơn vị thực hiện:

1. 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 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 của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: [ais@mic.gov.vn](mailto:ais@mic.gov.vn).

Trân trọng./.

### **Nơi nhận:**

- Như trên;
- Ban Giám đốc sở (báo cáo);
- Các đơn vị thuộc Sở;
- Lưu: VT, CNTT&BCVT

**KT. GIÁM ĐỐC  
PHÓ GIÁM ĐỐC**

**Nguyễn Văn Hiến**

**Phụ lục**  
**THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT**  
**TRONG SẢN PHẨM MICROSOFT**

(Kèm theo Công văn số /STTTT-CNTT&BCVT ngày / 12 /2022  
của Sở Thông tin và Truyền thông)

**1. Thông tin các lỗ hổng bảo mật**

| STT | CVE            | Mô tả  | Link tham khảo  |
|-----|----------------|--|---|
| 1   | CVE-2022-44698 | <ul style="list-style-type: none"> <li>- Điểm: CVSS: 5.4</li> <li>- Mô tả: lỗ hổng trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật. Lỗ hổng này đang bị khai thác trong thực tế.</li> <li>- Ảnh hưởng: Windows 10/11, Windows Server 2016/2019/2022.</li> </ul> | <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44698">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44698</a> |
| 2   | CVE-2022-41076 | <ul style="list-style-type: none"> <li>- Điểm CVSS: 8.5 (Cao)</li> <li>- Mô tả: lỗ hổng trong PowerShell cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022, PowerShell 7.2/7.3.</li> </ul>                                       | <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41076">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41076</a> |
| 3   | CVE-2022-44713 | <ul style="list-style-type: none"> <li>- Điểm CVSS: 7.5 (Cao)</li> <li>- Mô tả: lỗ hổng trong Microsoft Outlook for Mac cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing).</li> <li>- Ảnh hưởng: Microsoft Office 2019 for Mac, Office LTSC for Mac 2021.</li> </ul>                             | <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44713">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44713</a> |
| 4   | CVE-2022-44699 | <ul style="list-style-type: none"> <li>- Điểm CVSS: 5.5</li> <li>- Mô tả: lỗ hổng trong Azure Network Watcher Agent cho phép đối tượng tấn công thực hiện tấn công</li> </ul>  | <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44699">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44699</a> |

| STT | CVE                            | Mô tả   | Link tham khảo   |
|-----|--------------------------------|---|--|
|     |                                | <p>công vượt qua cơ chế bảo mật.</p> <ul style="list-style-type: none"> <li>- Ảnh hưởng: Azure Network Watcher Vm Extension.</li> </ul>   |  |
| 5   | CVE-2022-44710                 | <ul style="list-style-type: none"> <li>- Điểm CVSS: 7.8 (Cao)</li> <li>- Mô tả: lỗ hổng trong DirectX Graphics Kernel cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã có mã khai thác được công bố rộng rãi trên Internet.</li> <li>- Ảnh hưởng: Windows 11.</li> </ul>        | <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44710">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44710</a>  |
| 6   | CVE-2022-44678, CVE-2022-44681 | <ul style="list-style-type: none"> <li>- Điểm CVSS: 8.8 (Cao)</li> <li>- Mô tả: lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.</li> <li>- Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019.</li> </ul>                                 | <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44678">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44678</a><br><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44681">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44681</a> |
| 7   | CVE-2022-44690, CVE-2022-44693 | <ul style="list-style-type: none"> <li>- Điểm CVSS: 8.8 (Cao)</li> <li>- Mô tả: trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Microsoft SharePoint Server 2019, SharePoint Foundation 2013, SharePoint Enterprise Server 2013/2016.</li> </ul> | <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44690">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44690</a><br><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44693">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44693</a> |
| 8   | CVE-2022-44708, CVE-2022-41115 | <ul style="list-style-type: none"> <li>- Điểm CVSS: 8.3 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Microsoft Edge (Chromium-based) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.</li> </ul>  | <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44708">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44708</a><br><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41115">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41115</a> |

| STT | CVE            | Mô tả  | Link tham khảo  |
|-----|----------------|--|---|
|     |                | - Ảnh hưởng: Microsoft Edge  |   |
| 9   | CVE-2022-44673 | - Điểm CVSS: 7.0 (Cao)<br>- Mô tả: Lỗ hổng trong Windows Client Server Run-Time Subsystem (CSRSS) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.<br>- Ảnh hưởng: Windows 7/8.1/10, Windows Server 2008. | <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44673">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44673</a> |

## 2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng bảo mật 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/en-us>

<https://www.zerodayinitiative.com/blog/2022/12/13/the-december-2022-security-update-review>