

UBND TỈNH TÂY NINH  
**SỞ THÔNG TIN VÀ TRUYỀN THÔNG**

Số: /STTTT-TTGSĐH  
V/v cảnh báo lỗ hổng bảo mật có mức ảnh hưởng Cao trong các sản phẩm Microsoft công bố tháng 12/2022

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

Tây Ninh, ngày tháng 12 năm 2022

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các cơ quan tham mưu, giúp việc Tỉnh ủy;
- Mặt trận Tổ quốc và các Đoàn thể chính trị - xã hội;
- Các Sở, ban, ngành tỉnh;
- Các huyện, thị, thành ủy trực thuộc Tỉnh ủy;
- UBND các huyện, thị xã, thành phố;
- UBND các xã, phường, thị trấn.

Thực hiện theo Công văn số 2035/CATTT-NCSC của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2022 (***Thông tin chi tiết phụ lục kèm theo***).

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin cho người dùng, đơn vị và toàn bộ hệ thống của tỉnh, Sở Thông tin và Truyền thông đề nghị các đơn vị, địa phương thực hiện gấp các công việc cụ thể như sau:

1. Kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows và phần mềm có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời theo hướng dẫn tại phụ lục để tránh nguy cơ bị tấn công.

2. Tăng cường kiểm tra, giám sát hệ thống mạng của đơn vị, địa phương, khi có phát hiện hoạt động tấn công mạng, đề nghị liên hệ Sở Thông tin và Truyền thông để phối hợp xử lý kịp thời.

Thông tin liên quan đề nghị liên hệ Ông Vương Duy Thanh - Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung; Điện thoại: 0932624462.

Trân trọng./.

**Nơi nhận:**

- Như trên;
- GD Sở (b/c);
- P.CNTTBCVT;
- Lưu: VT, TTGSĐH.

**KT. GIÁM ĐỐC  
PHÓ GIÁM ĐỐC**

**PHỤ LỤC**  
**Thông tin các lỗ hổng nghiêm trọng trong các sản phẩm**  
**Microsoft công bố tháng 12/2022**

**1. Thông tin lỗ hổng bảo mật**

**- Mô tả:**

- 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.

**- Ảnh hưởng:**

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-44698	- Điểm: CVSS: 5.4 - 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.	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44698">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44698</a>

STT	CVE	Mô tả	Link tham khảo
		- Ảnh hưởng: Windows 10/11, Windows Server 2016/2019/2022.	
2	CVE-2022-41076	- Điểm CVSS: 8.5 (Cao) - Mô tả: lỗ hổng trong PowerShell cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022, PowerShell 7.2/7.3.	<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	- Điểm CVSS: 7.5 (Cao) - Mô tả: lỗ hổng trong Microsoft Outlook for Mac cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). - Ảnh hưởng: Microsoft Office 2019 for Mac, Office LTSC for Mac 2021.	<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	- Điểm CVSS: 5.5 - Mô tả: lỗ hổng trong Azure Network Watcher Agent cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật. - Ảnh hưởng: Azure Network Watcher Vm Extension.	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44699">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44699</a>
5	CVE-2022-44710	- Điểm CVSS: 7.8 (Cao) - 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. - Ảnh hưởng: Windows 11.	<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	- Điểm CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11, Windows	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44678">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44678</a> <a href="https://msrc.microsoft.com/update-">https://msrc.microsoft.com/update-</a>

STT	CVE	Mô tả	Link tham khảo
		Server 2008/2012/2016/2019.	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44681">guide/vulnerability/CVE-2022-44681</a>
7	CVE-2022-44690 CVE-2022-44693	- Điểm CVSS: 8.8 (Cao) - Mô tả: trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2019, SharePoint Foundation 2013, SharePoint Enterprise Server 2013/2016.	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44690">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44690</a> <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	- Điểm CVSS: 8.3 (Cao) - Mô tả: Lỗ hổng trong Microsoft Edge (Chromium-based) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Microsoft Edge	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44708">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44708</a> <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41115">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41115</a>
9	CVE-2022-44673	- Điểm CVSS: 7.0 (Cao) - Mô tả: Lỗ hổng trong Windows Client Server Runtime Subsystem (CSRSS) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - 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>

- **Đánh giá mức độ:** Đánh giá sơ bộ từ các chuyên gia bảo mật, lỗ hổng này ảnh hưởng đến nhiều thiết bị trên toàn cầu trong đó có cả Việt Nam. Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) đánh giá khả năng các mã khai thác của các lỗ hổng này sẽ sớm được công khai trên Internet trong thời gian sắp tới.

## 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. Nguồn tham khảo:**

<https://msrc.microsoft.com/update-guide/en-us>

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