Phụ lục

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

(Ban hành kèm theo văn bản số /STTTT-BCVT&CNTT 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	- 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. - Ảnh hưởng: Windows 10/11, Windows Server 2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44698
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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41076
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,	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44713

STT	CVE	Mô tả	Link tham khảo
		Office LTSC for Mac 2021.	
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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44699
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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44710
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 Server 2008/2012/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44678 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44681

STT	CVE	Mô tả	Link tham khảo
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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44690 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44693
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	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44708 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41115
9	CVE-2022-44673	- Điểm CVSS: 7.0 (Cao) - Mô tả: Lỗ hổng trong Windows Client Server Run-Time Subsystem (CSRSS) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 7/8.1/10, Windows Server 2008.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44673

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