Phụ lục

Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft

(Kèm theo Công văn số /CATTT-NCSC ngày / /2022 của Cục An toàn thông tin)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-26809	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong RPC Runtime Library cho phép đối tượng tấn công thực thi mã từ xa với đặc quyền cao trên hệ thống bị ảnh hưởng. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26809
2	CVE-2022-24491	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa với đặc quyền cao. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24491
3	CVE-2022-24497	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10, Windows Server 2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24497
4	CVE-2022-26815	- Điểm CVSS: 7.2 (cao) - Lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26815

		- Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022.	
5	CVE-2022-26904	- Điểm CVSS: 7.9 (cao) - Lỗ hổng trong Windows User Profile Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã có mã khai thác công khai trên Internet. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26904
6	CVE-2022-26919	- Điểm CVSS: 8.1 (Cao) - Lỗ hổng trong Windows LDAP cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26919
7	CVE-2022-24521	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Common Log File System Driver cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-24521

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/releaseNote/2022-Apr

https://www.zerodayinitiative.com/blog/2022/4/11/the-april-2022-security-update-review