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-2022-22047	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Client Server Run-Time Subsystem cho phép đối tượng tấn công thực hiện leo thang đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11. Windows Server 2008/2012.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22047
2	CVE-2022-30216	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Windows Server Service cho phép đối tượng tấn công cài chứng chỉ giả mạo độc hại lên máy chủ mục tiêu từ đó có thể thực hiện các dạng tấn công khác bao gồm tấn công chiếm quyền điều khiển. - Ảnh hưởng: Windows 10/11, Windows Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30216
3	CVE-2022-22029	- Điểm CVSS: 8.1 (Cao) - Lỗ hổng trong trong Windows Network File System cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22029
4	CVE-2022-22039	- Điểm CVSS: 7.5 (Cao) - Lỗ hổng trong trong Windows Network File System cho phép đối tượng tấn công không cần	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22039

		xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022.	
5	CVE-2022-22038	- Điểm CVSS: 8.1 (Cao) - Lỗ hổng trong trong Remote Procedure Call Runtime cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22038
6	CVE-2022-30206	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 7/8.1/10, Windows Server 2008/2012/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30206
7	CVE-2022-22022	- Điểm CVSS: 7.1 (Cao) - Lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2016/2019/2022.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22022
8	CVE-2022-30226	- Điểm CVSS: 7.1 (Cao) - Lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/12, Windows Server 2008/2012/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30226

9	CVE-2022-22041	- Điểm CVSS: 6.8 (Cao) - Lỗ hổng trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 8.1/10, Windows Server 2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22041

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-Jul

https://www.zerodayinitiative.com/blog/2022/7/12/the-july-2022-security-update-review