Phụ lục

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

(Kèm theo Công văn số: 2252/STTTT-TTCNS ngày 25/9/2023 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-36761	- Điểm: CVSS: 6.2 (Cao) - Mô tả: Lỗ hổng trong Microsoft Word cho phép đối tượng tấn công thu thập thông tin về mã băm NTLM của người dùng. Lỗ hổng này hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Word, Microsoft 365.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36761
2	CVE-2023-29332	- Điểm: CVSS: 7.5 (Nghiêm trọng) - Mô tả: Lỗ hổng trong dịch vụ Microsoft Azure Kubernetes Service cho phép đối tượng tấn công không cần xác thực thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Microsoft Azure Kubernetes Service.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29332
3	CVE-2023-38148	- Điểm: CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Internet Connection Sharing (ICS) cho phép đối tượng tấn công không cần xác thực thực thi mã từ xa khi ICS được kích hoạt. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38148
4	CVE-2023-36802	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Streaming Service Proxy cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng này hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36802

5	CVE-2023-38146	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Windows Themes cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38146
6	CVE-2023-36792 CVE-2023-36793 CVE-2023-36794 CVE-2023-36796	- Điểm: CVSS: 7.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Visual Studio cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft .NET Framework.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36792 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36793 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36794 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36796
7	CVE-2023-36744 CVE-2023-36745 CVE-2023-36756	- Điểm: CVSS: 8.0 (Cao) - Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Exchange Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36744 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36745 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36756

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. Các cơ quan, 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/ https://www.zerodayinitiative.com/blog/2023/9/12/the-september-2023-security-update-review