Phụ lục

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

(Kèm theo Công văn số: 2867 /STTTT-TTCNS ngày 23/11/2023 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-36397	- Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Pragmatic General Multicast cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36397
2	CVE-2023-36400	- Điểm: CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows HMAC Key Derivation cho phép đối tượng tấn công thực hiện leo thang đặc quyền. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36400
3	CVE-2023-36025	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công vượt qua tính năng bảo mật SmartScreen của Windows. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008,	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36025

STT	CVE	Mô tả	Link tham khảo
		2012, 2016, 2019, 2022.	
4	CVE-2023-36038	- Điểm: CVSS: 8.2 (Cao) - Mô tả: Lỗ hổng trong ASP.NET Core cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ (DoS). Thông tin chi tiết về lỗ hổng đã được công bố trong thực tế. - Ảnh hưởng: ASP.NET Core, .NET, Visual Studio 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36038
5	CVE-2023-36439	- 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 2016, 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36439
6	CVE-2023-36033	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows Desktop Manager cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36033
7	CVE-2023-36036	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows Cloud Files Mini Filter Driver cho phép đối tượng tấn công thực hiện leo thang đặc	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36036

STT	CVE	Mô tả	Link tham khảo
		quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2019, 2022.	
8	CVE-2023-36041	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Excel, Microsoft Office, Microsoft 365 Apps.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36041
9	CVE-2023-36413	- Điểm: CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công vượt qua tính năng bảo mật của Microsoft Office. Thông tin chi tiết về lỗ hổng đã được công bố trong thực tế. - Ảnh hưởng: Microsoft Office, Microsoft 365 Apps.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36413
10	CVE-2023-38177	- Điểm: CVSS: 6.1 (Cao) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2016, 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38177

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/2023/11/14/the-november-2023-security-update-review